Univerzita Karlova v Praze
Pedagogická fakulta

Katedra matematiky a didaktiky matematiky

Veronika Sedláčková

Gauss a konstruovatelnost pravidelných mnohoúhelníků pomocí kružítka a pravítka

Gauss and the constructability of regular polygons with ruler and compass

Bakalářská práce

Studijní program: Specializace v pedagogice

Studijní obor: Matematika se zaměřením na vzdělávání – jednooborové studium

Vedoucí práce: prof. RNDr. Ladislav Kvasz, Dr.

Praha 2014

Čestné prohlášení

Prohlašuji, že jsem závěrečnou práci vypracovala pod vedením vedoucího práce samostatně a citovala všechny použité prameny a literaturu.

Dále prohlašuji, že práce nebyla využita k získání jiného nebo stejného titulu.

Souhlasím s trvalým uložením elektronické verze mé práce v databázi meziuniverzitního projektu Theses.cz za účelem soustavné kontroly podobnosti kvalifikačních prací.

V Praze 11. dubna 2014

……

Veronika Sedláčková

Poděkování

Na tomto místě bych ráda poděkovala zejména mému vedoucímu práce, prof. RNDr. Ladislavu Kvaszovi, Dr. za konzultace, užitečné rady a odborné vedení mé bakalářské práce. Dále bych chtěla poděkovat celé mé rodině za velkou trpělivost a podporu.

ABSTRAKT

Bakalářská práce se zabývá vybranými euklidovskými konstrukcemi pravidelných mnohoúhelníků a shrnuje jejich historický vývoj. Zaměřuje se zejména na matematika, který je s tímto tématem neodmyslitelně spjat, tedy na Carla Friedricha Gausse. V první části práce jsou podány důležité údaje z Gaussova života a zejména pak z jeho vědeckých děl. Poté je zde algebraicky charakterizován pojem konstruovatelnosti kružítkem a pravítkem, jsou dokázány důležité věty, na kterých jsou tyto konstrukce založeny.

Dále je vyslovena a dokázána Gaussova věta o konstruovatelnosti pravidelných mnohoúhelníků a to za použití Galoisovy teorie.

Další část je zaměřena na Gaussovu konstrukci pravidelného 17-úhelníka, která je zde detailně popsána. Zároveň jsou vysvětleny některé další zajímavé konstrukce od různých autorů, které vznikaly v průběhu 19. a počátkem 20. století.

KLÍČOVÁ SLOVA

Carl Friedrich Gauss, euklidovské konstrukce, pravidelné mnohoúhelníky, Galoisova teorie

ABSTRACT

The bachelor thesis deals with chosen Euclidean constructions of regular polygons and summarizes their historical development. It focuses on the mathematician who is essentially adherent to this theme, his name is Carl Friedrich Gauss. In the first part of the thesis the important statements from Gauss's life and particularly from his scientific publications are given. Then the idea of algebraic formulation of the constructions with ruler and compass is characterized and the main theorems about these constructions are proved here.

Further Gauss's theorem about constructability of regular polygons is given and proved while using Galois Theory.

The next part is focused on Gauss's construction of the regular 17-gon, which is described in details. At the same time the thesis explains other interesting constructions from various authors created during the 19^{th} century and in the beginning of the 20^{th} century.

KEYWORDS

Carl Friedrich Gauss, Euclidean constructions, regular polygons, Galois Theory

Obsah

Úvod

Mnohé matematické definice, věty a tvrzení se nazývají podle autora, který je poprvé vyslovil. Při studiu matematiky tak narazíme na Fermatova prvočísla, Eulerovu větu, Eukleidovské konstrukce, Gaussovu větu, apod. Většina z nás se naučí název věty, ale dál se už nezajímá o autora, o pozadí, kdy a za jakých podmínek na toto tvrzení přišel, jaké skutečnosti ho vedly k tomu, aby se danou otázkou zabýval, jaké jsou souvislosti s další autorovou činností, jaké je historické pozadí, atd. Právě tyto otázky a mnohé další spojené s životem významných matematiků jsou jistě velice zajímavé. Pro bakalářskou práci jsme vybrali jednoho z největších matematiků, Carla Friedricha Gausse. Pokud bychom se ale měli do hloubky zabývat celou matematickou činností tohoto velikána, vydalo by to na několik bakalářských prací. Zaměříme se proto pouze na pravidelné mnohoúhelníky, zejména pak na konstrukci pravidelného 17-úhelníku, na kterou byl Gauss natolik pyšný, že si přál, aby měl pravidelný 17-úhelník na svém náhrobku.

Cílem práce je dokázat větu vymezující konstruovatelné pravidelné mnohoúhelníky, vysvětlit Gaussovu konstrukci pravidelného 17-úhelníku a popsat některé další konstrukce od jiných autorů. Zároveň podáme i historické souvislosti, ve kterých tyto konstrukce vznikaly, zaměříme se zejména na život Carla Friedricha Gausse.

V první části práce podáme stručný Gaussův životopis, poté se budeme zabývat jeho činností v různých vědeckých oblastech. Dále si vysvětlíme pojem konstruovatelnosti kružítkem a pravítkem a vyslovíme a dokážeme Gaussovu větu.

V druhé části se zaměříme na konstrukce pravidelného 17-úhelníku, popisované postupy doplníme o názorné obrázky, které jsou vytvořeny v programu Geogebra.

Při hledání a zpracovávání různých zdrojů pro téma konstrukcí pravidelného 17-úhelníku jsme se přesvědčili, že i v dnešní době probíhá celá řada diskusí o tom, která konstrukce tohoto mnohoúhelníku je nejelegantnější, nejzajímavější, nebo která má nejméně kroků, a stále se hledají různé neobvyklé způsoby při jeho sestrojování. Je tedy patrné, že otázka konstrukce pravidelného 17-úhelníku, je i po téměř dvě stě letech od Gaussova důkazu konstruovatelnosti stále aktuálním tématem.

Při své práci jsem čerpala jednak z historických děl (Gauss, Strnad, Studnička, Rychlík), pak z učebnic algebry (Stewart, Kořínek) a populárních textů (Courant, Bühler, Archibald a Tietze).

1 Eukleidovské konstrukce pravidelných mnohoúhelníků

1.1 Základní pojmy

Nejdříve si zavedeme základní pojmy, ze kterých budeme dále vycházet.

1.1.1 Eukleidovské konstrukce

V celé práci se budeme zabývat eukleidovskou konstrukcí, tedy konstrukcí, při níž používáme pouze rovné pravítko a kružítko, přičemž i ty nejsložitější konstrukce vytváříme postupným využitím dvou základních úkonů (Kořínek 1956, s. 465):

1. Jsou-li dány dva body, spojit tyto body přímkou.
2. Je-li dán bod a délka úsečky, sestrojit kružnici o středu v daném bodě a poloměru rovnému délce úsečky.

Pokud chceme konstruktivní úlohu řešit eukleidovsky, znamená to z bodů 1 a 2 vytvářet postupně další body, které splňují zadání dané úlohy. Využitím konstrukcí 1 a 2 s pomocí terminologie moderní matematiky tedy dokážeme najít tyto body:

1. Průsečík dvou přímek.
2. Průsečík přímky a kružnice.
3. Průsečík dvou kružnic.

Nyní si zavedeme pravoúhlou souřadnicovou soustavu v rovině. Pro souřadnice daných bodů pak platí následující vztahy:

Věta: Jestliže lze danou úlohu vyřešit eukleidovsky, pak souřadnice hledaných bodů lze vypočítat ze souřadnic zadaných bodů použitím racionálních operací, tedy součtu, rozdílu, součinu a podílu a dále pak výpočtu druhé odmocniny.

Platí i věta obrácená.

Věta: Pokud se dají vypočítat souřadnice hledaného bodu pomocí racionálních operací a pomocí druhé odmocniny ze souřadnic zadaných bodů, pak lze tento bod sestrojit eukleidovsky.

Důkazy obou vět jsou uvedeny v knize (Kořínek 1956, s. 467–469).

1.1.2 Pravidelný mnohoúhelník

Definici mnohoúhelníku najdeme téměř v každé učebnici matematiky pro střední školy, jednotlivá zavedení jsou v zásadě velmi podobná. Polák ve své knize (Polák 2008, s. 448) definuje mnohoúhelník následovně: „Nechť je dáno *n* takových úseček A_1A_2, A_2A_3, $A_3A_4, \dots, A_{n-1}A_n$ $(n \in N, n \geq 3)$, že každé dvě sousední úsečky mají společný právě jeden krajní bod a neleží v téže přímce. Pak sjednocení množiny všech úseček A_1A_2, A_2A_3, $A_3A_4, \dots, A_{n-1}A_n$ […] nazýváme lomenou čarou $A_1A_2 \dots A_{n-1}A_n$. Uzavřená lomená čára $A_1A_2 \dots A_{n-1}A_1$, jež leží v rovině a sama sebe neprotíná […], ohraničuje část roviny, která se nazývá ***mnohoúhelník*** či určitěji ***n-úhelník*** $A_1A_2 \dots A_{n-1}A_n$ […].“

Pravidelné mnohoúhelníky jsou pak speciální skupinou konvexních mnohoúhelníků: **„*Pravidelný mnohoúhelník*** je každý mnohoúhelník, jehož všechny strany a všechny vnitřní (a tedy i vnější) úhly jsou shodné. Každý pravidelný *n*-úhelník je tětivový i tečnový, opsaná i vepsaná kružnice mají společný střed, který se nazývá střed pravidelného mnohoúhelníku,“ (Polák 2008, s. 450).

Dále v textu budeme používat jednotkovou kružnici opsanou *n*-úhelníku se středem v počátku souřadnic.

1.1.3 Eukleidovské konstrukce pravidelných mnohoúhelníků

Praktická geometrie využívala konstrukci základních pravidelných mnohoúhelníků již dávno před Euklidem. Petr Vopěnka vytvořil v (Eukleides 2007) *hypotetickou příručku pro napínače provazů*, kteří používali tyto konstrukce pro vyměření různých pozemků a staveb. „Zachycovali je značkami (body), které umisťovali do vrcholů (rohů), popřípadě některých dalších významných míst vytyčovaných útvarů,“ (Eukleides 2007, s. 13).

Jedním z prvních matematiků, který se konstrukcemi pravidelných mnohoúhelníků zabýval a který sepsal do té doby známé konstrukce, byl *Eukleides z Alexandrie* (asi 365–280). Ve svých *Základech* popisuje konstrukci pravidelného trojúhelníku, čtverce, pravidelného pětiúhelníku, šestiúhelníku a patnáctiúhelníku, přičemž při konstrukci patnáctiúhelníku využívá konstrukci pravidelného trojúhelníku a pětiúhelníku. Postupným půlením počtu stran byl Eukleides schopen sestrojit další pravidelné *n*-úhelníky. Tietze je shrnul do následujícího přehledu (Tietze 1965, s. 187):

$$n = 4, 8, 16, 32, 64, \cdots,$$
$$n = 3, 6, 12, 24, 48, \cdots,$$
$$n = 5, 10, 20, 40, 80, \cdots,$$
$$n = 15, 30, 60, 120, 240, \cdots.$$

Eukleides tedy věděl, že pravidelný *n*-úhelník lze zkonstruovat pomocí pravítka a kružítka, když $n = 2^i 3^j 5^k$, kde $n \geq 3, i \geq 0$, jsou celá čísla a $j, k \in \{0,1\}$ (Křížek 2001, s. 179). Přesnou konstrukci pravidelného *n*-úhelníku s počtem stran $7, 9, 11, 13, 17, \cdots$ nebyl Eukleides schopen sestrojit.

Téměř dva tisíce let nikoho ani nenapadlo zabývat se možnými konstrukcemi dalších mnohoúhelníků, neboť všichni věřili, že v antické době vyčerpali všechny možné konstrukce. Až 1. června v roce 1796 poslal profesor E. A. W. Zimmermann stručné oznámení[1] do časopisu *Intelligenzblatt der allgemeinen Litteraturzeitung*, které vyšlo ve sloupku *Neue Entdeckungen (Nové objevy)*, o tom, že ***Carl Friedrich Gauss*** objevil konstrukci pravidelného 17-úhelníku. Tento objev rozpoutal v matematických kruzích senzaci a spustil vlnu dalších možných konstrukcí pravidelných mnohoúhelníků. Do dnešní doby byla popsána celá řada konstrukcí pravidelného 17-úhelníku, některé z nich popíšeme v kapitole 2.

Julius Friedrich Richelot (1808–1875) popsal na 194 stranách konstrukci pravidelného 257-úhelníku, vyšla nejprve v roce 1832 ve čtyřech částech v časopise *Journal für die reine und angewandte Mathematik* v článku pod názvem *De resolutione algebraica aequationis* $x^{257} = 1$*, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata*.

Johann Gustav Hermes (1846–1912) provedl konstrukci pravidelného 65 537-úhelníku, pracoval na ní 10 let, celý jeho popis je uložen na univerzitě v Göttingenu, v oddělení matematiky, jak o tom píše Tietze ve své knize *Famous Problems of Mathematics* (Tietze 1965, s. 192).

[1] Pod názvem „C. F. Gauss z Brunšviku, student matematiky v Göttingenu“, Zimmermann dále píše: „Zaslouží si zmínku, že pan Gauss se nyní ve svých 18 letech věnuje zde v Brunšviku filozofii a klasické literatuře se stejně velkým úspěchem jako ve vyšší matematice“ (Tietze 1965, s. 204).

2 Carl Friedrich Gauss

2.1 Gaussův životopis

Johann Carl Friedrich Gauss se narodil 30. dubna 1777 v Brunšviku, kam se přestěhovali Gaussovi prarodiče, původně drobní farmáři. Gaussův otec, Gebhard Dietrich Gauss (1744–1808), nemohl jako přistěhovalec najít adekvátní práci, nejdříve pracoval jako zahradník, poté jako pouliční řezník a později jako účetní a pokladník pohřební společnosti. Uměl číst, psát a dobře ovládal základní aritmetiku. Jeho matka, Dorothea Gauss[2] (1745–1842) uměla číst, ale neuměla prý psát. Podle vlastních slov měl Gauss blíž ke své matce, o kterou se posledních 22 let jejího života láskyplně staral. Později svůj geniální talent přisuzoval právě rodině své matky (Bühler 1987, s. 6).

O Gaussově raném dětství se traduje několik historek ohledně jeho brzké geniality. Již ve třech letech uměl Gauss výborně počítat, jedna z historek vypráví, že opravil svého otce při výpočtu mzdy pro najaté zedníky za práci konanou přes čas. Ještě než nastoupil v roce 1784 na základní školu, naučil se prý sám číst a psát. Sám Gauss o sobě později vyprávěl, že prý uměl dřív počítat než mluvit (Studnička 1877, s. 150).

2.1.1 Studium

Na základní škole měl neobvyklé štěstí na svého učitele, J. G. Büttnera, který velice brzy rozpoznal Gaussův matematický talent a objednal mu z Hamburku speciální aritmetickou knihu, protože si uvědomil, že sám ho ničemu novému už naučit nemůže (Bühler 1987, s. 7). Během těchto let se mladý Gauss spřátelil s Büttnerovým pomocníkem, Johannem Christianem Martinem Bartelsem (1769–1836). O 8 let starší Bartels Gaussovi půjčoval různé knihy a všemožně ho podporoval i v dalším životě. Sám Bartels se později stal profesorem matematiky na univerzitě v Kazani. V roce 1788 pomohl Büttner Gaussovi s přijetím do druhého ročníku na gymnázium, kde se Gauss naučil spisovnou němčinu a velmi dobře latinsky. V roce 1792 byl přijat na prestižní akademii *Collegium Carolinum*, kde se ještě dále zdokonaloval v latině a řečtině, což bylo v té době velmi důležité pro jeho pozdější akademickou činnost (latinu hojně využil i ve svých spisech). Díky velmi dobré místní knihovně si mohl prostudovat mnoho klasických matematických spisů, zejména Newtonových, Eulerových a Lagrangeových (Studnička 1877, s. 152). Při svém vzdělávání měl

[2] Její rodné příjmení bylo Bentze.

Gauss velké štěstí na osoby kolem sebe, neboť dalším Gaussovým podporovatelem byl státní rada a profesor na akademii *Collegium Carolinum*, E. A. W. Zimmermann, díky němuž Gausse po dlouhá léta velmi dobře finančně zabezpečoval brunšvický vévoda Karel Vilém Ferdinand a sám Gauss se tak mohl plně věnovat studiu. V roce 1795 vyslovil Gauss pomocí indukce fundamentální poučku o kvadratických zbytcích, z jeho deníku víme, že v té době se nejvíce zajímal o teorii čísel a algebru, přesto v roce 1795 začal studovat klasickou filologii na univerzitě v Göttingenu. Ale již 30. března 1796, kdy objevil konstrukci pravidelného 17-úhelníku, své rozhodnutí změnil a od té doby se plně věnoval studiu matematiky. Na univerzitě se spřátelil s maďarským šlechticem Wolfgangem von Bolyai (1775–1856), který zde studoval filozofii. Roku 1798 odchází Gauss z univerzity, aniž by získal titul, doktorskou disertaci dokončil později na Helmstedtské univerzitě r. 1799. Předmětem jeho disertace byl důkaz *fundamentální věty algebry*, která tvrdí, že každý nekonstantní polynom s komplexními koeficienty má alespoň jeden komplexní kořen (Kořínek 1956, s. 354). Později tuto větu dokázal ještě jinými způsoby, v prosinci 1815, v lednu 1816 a v roce 1849, kdy svůj poslední důkaz předvedl na univerzitě v Göttingenu při oslavě padesátiletého výročí od získání svého doktorátu.

2.1.2 Rodina, sociální zázemí a politické pozadí.

V rodinném životě nastává změna r. 1805, kdy se Gauss oženil s o 3 roky mladší Johannou Osthofovou. Z korespondence mezi Gaussem a jeho budoucí ženou víme, že ji Gauss upřímně miloval, ale v dopise Bolyaimu z 25. listopadu 1804 si Gauss dělá starosti ohledně života se svojí nastávající ženou, která je úplně jiná než on, „inteligentní a milá, ale také nezkušená a ne moc dobře vzdělaná“ (Bühler 1987, s. 49). Po třech letech manželství je z jeho korespondence patrné, že ho rodinný život naplňuje a že je velice šťastný. V dopise z 2. září 1808, který byl opět adresován Bolyaimu, se Gauss svěřuje: „ Když dceři vyroste nový zub, nebo když se syn naučí nová slůvka, pak je to téměř stejně důležité jako objev nové hvězdy nebo nové pravdy…“ (Bühler 1987, s. 66). Do r. 1806 žil Gauss spokojeně ve svém rodném městě, neustále podporován vévodou z Brunšviku, mohl se tedy plně věnovat svým výzkumům, neměl žádné jiné povinnosti. V roce 1807 ale nastává zvrat, do Gaussova života zasahují dvě důležité události. Zásluhou svého dlouholetého přítele, německého astronoma, lékaře a fyzika, Heinricha Wilhelma Olberse (1758–1840), byl Gauss jmenován profesorem astronomie a ředitelem hvězdárny v Göttingenu, kde

působil až do konce svého života. Několikrát se sice snažili Gausse povolat do jiných měst, nabízeli mu zajímavé pozice v Petrohradu, Berlíně i Vídni, on však zůstával v Göttingenu, neboť tam byl šťastný a líbilo se mu tam. Díky němu byla tamější hvězdárna vybavena nejnovějšími přístroji a byla kompletně přebudována.

Na druhé straně Gauss přestal být finančně podporován vévodou Ferdinandem, který byl zabit v bitvě u Jeny r. 1806, když vedl pruskou armádu proti Napoleonovi. Do této doby byl Brunšvik součástí státu Hannover, ale po prohrané bitvě se stal součástí nově vytvořeného Vestfálského království, včele s nejmladším bratrem Napoleona. Později, v r. 1811, si Hannover zcela podrobila Francie. Podle knihy *Famous Problems of Mathematics* (Tietze 1965, s. 196) prožíval Gauss v těchto letech velmi těžké období, lidé museli platit velké daně a mnoho dalších poplatků. Tietze o těchto událostech píše: „Pro jeho rodinu bylo velmi obtížné pochopit člověka, který se uprostřed strádání a trápení totálně ponořil do svého světa pojmů. Dokonce si mysleli, že se pomátl. (Tietze 1965, s. 196) Po jeho smrti se ale našlo uprostřed matematického náčrtu napsáno: „Smrt je vhodnější pro tento způsob života.“ (Tietze 1965, s. 196) Gauss tedy sice působil dojmem, že ho nastalá situace v zemi nezajímá, neprojevoval veřejně své politické názory, ani se nikterak neangažoval, naopak se zcela uzavřel do světa vědy, z jeho poznámek je ale patrné, že se i jeho vzniklé útrapy dotýkají.

V této době ho bohužel stíhá ještě další rána, r. 1809 umírá jeho manželka Johanna při porodu jejich třetího syna a krátce poté i jeho syn Louis. Gauss propadl depresím, ze kterých se už nikdy úplně nevyléčil. Nicméně rok nato se znovu oženil, s přítelkyní své první ženy Friederic Wilhelmine Waldeckovou, které všichni říkali Minna. Toto manželství ale nebylo příliš šťastné, neboť bylo poznamenáno častými nemocemi Minny a později také stálými konflikty Gausse se syny Eugenem a Wilhelmem. Oba synové vyřešili problémy se svým otcem emigrací do Severní Ameriky, Eugen se usadil v Missouri, Wilhelm v St. Louis. Se svým otcem už se nikdy neviděli, později si s ním alespoň korespondovali. Minna nakonec r. 1831 po vleklé nemoci zemřela a o Gausse se až do jeho smrti starala jeho mladší dcera Theresa. Gauss měl celkem 6 dětí, s Johannou měl Josepha (1806–1873), Wilhelminu (1808–1846), Louise (1809–1810), s Minnou měl Eugena (1811–1896), Wilhelma (1813–1879) a Theresu (1816–1864). Joseph dostal jméno podle astronoma Piazziho,

který objevil Ceres, Wilhelmina podle Olberse, jemuž vděčíme za objev planetky Pallas a Louise se jmenoval podle Hardinga, objevitele planetky Juno.

V Göttingenu Gauss působil i jako profesor astronomie, navzdory svému veřejnému prohlašování, že samotným vyučováním pohrdá a že ho učit nebaví. Bühler ve své knize (Bühler 1987, s. 71) vysvětluje, že ve skutečnosti ale Gauss odmítal pouze způsob, jakým se v té době vedla výuka, chtěl od svých studentů, aby pracovali a mysleli nezávisle, byl přesvědčen, že pro jejich úspěšné studium je mnohem důležitější vlastní úsilí, než pouhé vysvětlování od profesora. Byl znechucen, když viděl, že většina studentů neprojevovala žádný zájem, neměla téměř žádnou motivaci, dokonce ani valné vědomosti. Na druhé straně byl rád, když mohl poradit každému studentu, který se aktivně zajímal o získávání nových poznatků. Jak píše Bühler, můžeme se o tom přesvědčit opět z Gaussových dopisů: „Existuje mnoho příkladů v korespondenci se Schumacherem, které ukazují, že Gaussovi nevadilo vysvětlovat různé věci do detailů a opakovaně.“ (Bühler 1987, s. 71) Ve stylu, jakým Gauss psal své spisy, je rovněž patrná jeho snaha o čtenářovo pochopení jeho myšlenek a pojmů. Důkazem je velké množství příkladů, které Gauss zařadil do svých knih a také jeho hledání co nejlogičtějších cest ve svých argumentacích. Na druhou stranu víme, že mnoho Gaussových současníků shledalo jeho práce příliš obtížné a nemotivující (Bühler 1987, s. 71).

2.1.3 Na sklonku života

Gauss se do konce svého života nepřestával vzdělávat, každý den chodil na dvě hodiny do knihovny, kde „udržoval spojení se všemi svými známými, jakož i pomocí novin s ostatním světem.“ (Studnička 1877, s. 15)

Zemřel po nemoci srdce, 23. února 1854 v 1 hodinu a 5 minut. Byl pohřben v Göttingenu. Kniha *Gauss: A Biographical Study* popisuje, že smutečního obřadu se zúčastnila celá řada významných osobností, jeho zeť se o něm ve svém smutečním projevu vyjádřil jako o výjimečném géniovi, kterému se nikdo nevyrovnal. Jedním z těch, kdo nesli rakev, byl Richard Dedekind, v té době 24 letý student matematiky (Bühler 1987, s. 155). Když Gauss zemřel, „na jeho počest mu vládnoucí hannoverský král nechal zhotovit medaili, která ho oslavovala jako prince matematiky.“ (Tietze 1965, s. 198) Roku 1880 mu v Brunšviku postavili památník, jehož základem je pravidelný 17-úhelník.

Felix Klein prohlásil o Gaussovi na jedné ze svých přednášek o vývoji matematiky v 19. století: „Měl pouze dva velikány, s kterými se mohl rovnat, Archimeda a Newtona, jež byli stejně nadaní jako on.“ (Klein 1979, s. 198)

2.2 Přehled o Gaussově díle

2.2.1 Matematika

Od roku 1795 začal Gauss sestavovat svůj velkolepý spis *Disquisitiones arithmeticae (Aritmetické výzkumy)*, který vydal po několika nesnázích v létě r. 1801 v Lipsku a který věnoval svému mecenáši, vévodu Ferdinandovi[3]. Tato kniha zavedla teorii čísel jako matematickou disciplínu. Není samozřejmě jediným matematickým dílem, které Gauss vydal, ale svým významem je rozhodně stěžejní. Budeme se mu proto věnovat podrobněji. Celá kniha je rozdělena do 7 kapitol:

Kapitola I: Numerorum congruentia in genere (kongruentní čísla obecně), 5 stran
Kapitola II: Congruentiis primi gradus (kongruence prvního stupně), 24 stran
Kapitola III: De Residuis potestatum (zbytkové třídy), 35 stran
Kapitola IV: De congruentiis secundi gradus (kongruence druhého stupně), 47 stran
Kapitola V: De formis aequationibusque indeterminatis secundi gradu (formy neurčitých rovnic druhého stupně), 260 stran
Kapitola VI: Variae applicationes disquisitionum praecedentium (různé aplikace předchozích rozprav), 32 stran
Kapitola VII: De aequationibus, circuli sectiones definientibus (rovnice definující části kruhu), 53 stran

Nyní se pokusíme stručně popsat náplň jednotlivých částí, vycházíme z knihy (Bühler 1987).

Kapitoly I – III jsou úvodní, Gauss zde shrnul dosavadní poznatky o základech teorie čísel, byl první, kdo je systematicky utřídil do uceleného celku, zároveň však přidal i některá svá vlastní tvrzení a důkazy. V kapitole II zavádí symbol $a \equiv b \; mod \; c$ pro kongruenci, samotný pojem byl již ale znám dříve.

[3] Kniha byla vydána na jeho náklady.

Hlavní částí knihy jsou kapitoly IV a V. Nejdůležitějším předmětem kapitoly IV je pojem kvadratické reciprocity. Tímto tématem se již zabývali Euler a Legendre, ale Gauss zde podává první korektní důkaz[4]. Ústřední částí je pak kapitola V, která je zároveň nejobsáhlejším úsekem. Gauss zde pojednává o teorii binárních a ternárních kvadratických forem, navazuje zde na práci Lagrangea, jehož výsledky na začátku této části shrnuje. V kapitole VI Gauss představuje některé aplikace pojmů, které podal v oddíle V.

Kapitola VII je nejpopulárnější součástí knihy, zejména pak dělení kruhu pomocí pravítka a kružítka a popis konstrukce pravidelného 17-úhelníku. Tato část je dalším tématem bakalářské práce, budeme se jí podrobněji zabývat později.

Gaussova matematická činnost se stala základem pro rozvoj mnoha dalších teorií. Mezi významné matematiky, kteří z jeho myšlenek čerpali a navazovali na jeho práci, patřil např. *Peter Gustav Lejeune Dirichlet* (1805–1859), *Ernst Eduard Kummer* (1810–1893), *Bernhard Riemann* (1826–1866), *Richard Dedekind* (1831–1916), *Hermann Minkowski* (1864–1909) a mnozí další. Bühler píše o vlivu Gaussovy aritmetické práce: „Spis *Disquisitiones arithmeticae* a Gaussovy další spisy o teorii čísel, včetně mnoha těch, které byly vydány posmrtně, měl ohromný a trvalý vliv na rozvoj teorie čísel v 19. století a v první polovině 20. století. […] Proč hrály Gaussovy myšlenky takovou zásadní roli je jednoduché. Gaussův dominantní zájem o konkrétní problémy a jeho nechuť používat abstraktní pojmy ho vedly k vytvoření ideálních nástrojů pro jeho teoretický přehled starších výsledků a k objevení tak bohaté škály pojmů nových.“ (Bühler 1987, s. 36)

Studnička píše, že kniha *Disquisitiones arithmeticae* Gaussovi nepřinesla zasloužené uznání, jednak kvůli malému počtu vydaných knih[5], hlavně ale také proto, že v té době bylo málo matematiků, kteří byli schopni spisu porozumět a proniknout do hloubky samotných matematických pojmů (Studnička 1877, s. 155).

2.2.2 Astronomie

Veřejnou slávu a uznání Gaussovi zaručila až astronomie, když ve svých 24 letech předpověděl pozici trpasličí planetky Ceres. Původně ji objevil italský astronom Piazzi, ale později už ji nemohl nikdo najít. Podařilo se to až Gaussovi a to zcela na

[4] Celkem toto pravidlo dokázal 6 různými způsoby, z toho dva jsou v knize *Disquisitiones arithmeticae*.
[5] Úpadkem pařížského prodejce se ztratila velká část nákladu.

jiném místě, daleko od pozice, kterou původně předpovídaly předchozí primitivní metody. Gauss tak vytvořil mnohem jednodušší metody pro výpočty drah těles ve vesmíru (Bühler 1987, s. 43–44). Svoje myšlenky shrnul roku 1809 v díle *Theoria motus corporum coelestium in sectionibus conicis circa Solem ambientium (Teorie pohybu nebeských těles obíhajících po eliptických dráhách kolem slunce)*. Stejně jako *Disquisitiones arithmeticae* je celá kniha sepsána v latině[6], na poli astronomie měla ohromný význam. Spis rovněž obsahuje i *metodu nejmenších čtverců*[7], která se dodnes používá v různých odvětvích vědy k minimalizaci chyby měření. Za svoje významné dílo získal Gauss uznání a obdiv celé astronomické společnosti, byl oceněn mnohými medailemi a diplomy.

2.2.3 Fyzika a geodézie

Roku 1816 pověřila vláda Hannoverského království[8] Gausse, aby vytvořil geodetický výzkum Hannoveru, měl tak následovat svého dlouholetého přítele Heinricha Christiana Schumachera (1780–1850), který provedl nejdříve triangulaci Holsteinu a později pak celého Dánska. Pro Gausse to byl úkol, který trval téměř 25 let. Výsledky této činnosti vedly nejen k vytvoření spolehlivých map, ale také k získání znalostí přesného tvaru země. Jak píše Tietze, Gauss v této oblasti nejen, že vynalezl výpočetní techniky, které se v geodézii používají dodnes, ale také vynalezl heliotrop, přístroj, který odráží sluneční paprsky na velkou vzdálenost a pomáhá tak určit přesnou pozici (Tietze 1965, s. 196).

Na jedné cestě do Berlína se Gauss seznámil s fyzikem Wilhelmem Webrem, kterého pak v r. 1831 povolal do Göttingenu, aby zde působil jako profesor fyziky. Gausse Webrova práce, zejména pak jeho magneticko-elektrické experimenty, zaujaly natolik, že se pustil s Webrem do spolupráce[9]. R. 1832 vyšlo podle (Seydler 1877, s. 192) „pojednání o absolutním měření intensity zemského magnetismu“: *Intensitas vis magneticae terrestris ad mensuram absolutam revocata*. R. 1834 zkonstruovali Gauss s Weberem první elektromagnetický telegraf, který spojoval hvězdárnu a institut fyziky v Göttingenu. Téhož roku se zasloužili o založení *magnetického*

[6] Původně ji Gauss napsal německy, ale po naléhání nakladatele, aby ji kvůli většímu prodeji napsal francouzsky, se Gauss rozhodl, že ji přeloží do latiny (vedly ho k tomu zřejmě vlastenecké důvody).
[7] Legendre tuto metodu publikoval již dříve, ale Gauss tvrdil, že ji použil jako první, a sice pro výpočet dráhy planetky Ceres (Bühler 1987, s. 138).
[8] Po opětovném nastolení míru byl Hannover r. 1815 po Kongresu ve Vídni prohlášen znovu za království.
[9] Gauss se o fyziku, zejména teoretickou, zabýval již dříve, vydal několik spisů ještě před spoluprací s Weberem.

spolku, jenž podporoval měření zemského magnetismu v různých částech světa. Díky Gaussovi byla v Göttingenu vybudována magnetická observatoř[10], jeho zásluhou byl také publikován atlas geomagnetismu. Göttingen se tak stává uznávaným centrem mezinárodního výzkumu v této oblasti (Bühler 1987, s. 128). Roku 1839 vydává Gauss své třetí stěžejní dílo zvané *Allgemeine Theorie des Erdmagnetismus (Všeobecná teorie zemského magnetismu)*.

2.2.4 Gaussovy sebrané práce

Pod vedením Felixe Kleina (1849–1925) vyšlo během let 1863–1929 12 svazků pod názvem *Carl Friedrich Gauss'Werke*. 8 svazků shrnuje Gaussovu vědeckou práci v matematice, astronomii, geodézii a fyzice. Další svazky obsahují různé nedokončené studie, eseje, náčrty a fragmenty, které Gauss nikdy neplánoval vydat, dále jeho korespondenci, ale i „rozsáhlé a detailní eseje od kompetentních matematiků a vědců, kteří posuzovali Gaussův přínos do oborů, ve kterých pracoval" (Bühler 1987, s. 18). Ve sbírce je zařazen i Gaussův matematický deník, který si vedl v letech 1796–1801[11], díky němuž můžeme poměrně přesně datovat některé výsledky jeho matematické práce. První zápis je o konstrukci pravidelného 17-úhelníku. (Bühler 1987, s. 19)

Gauss nechával značné množství věcí, na které přišel, ležet v zásuvce ve stole a nepublikoval je, často se stávalo, že na ně pak přišel někdo jiný, a když mu chtěli oznámit svůj objev, často slýchávali: „Tyto věci pro mě nejsou nové." (Tietze 1965, s. 198) Až po jeho smrti, když se vydávala sbírka jeho prací, našla se velká část těchto zápisků. Mnohdy Gauss šetřil papírem a vpisoval si své vlastní poznámky na okraje a prázdné stránky do knihy o aritmetice, jejíž autor byl *Leiste* (Bühler 1987, s. 19).

2.3 Gaussova věta

2.3.1 Zavedení

Roku 1796 1. června napsal Gauss do časopisu *Intelligenzblatt der allgemeinen Litteraturzeitung* o svém objevu konstrukce pravidelného 17-úhelníku: „Tento objev

[10] Podle vzoru Humboldtovy observatoře v Berlíně.
[11] Končí až r. 1814, ale pravidelně si Gauss zapisoval do r. 1801.

je jen důsledkem teorie s daleko větším obsahem, která ještě není úplná, ale kterou hned vydám, jakmile bude dokončena.“ (Archibald 1920, s. 324) Význam jeho prohlášení byl patrný až v roce 1801, kdy vydal *Disquisitiones arithmeticae*. V tomto spisu (Kapitola VII, body 365 a 366) stanovil nutné a postačující podmínky pro konstruovatelnost pravidelných *n*-úhelníků, dokázal zde podmínku postačující, nutnou podmínku ale nikdy nepublikoval (Stewart 2004, s. 209). V roce 1837 ji dokázal francouzský matematik Pierre Wantzel (1814–1848). (Křížek 2001, s. 180) Když Gauss uvažoval, který pravidelný mnohoúhelník lze sestrojit a který nikoli, vyřešil geometrický problém dělení kruhu na *n* stejných dílů algebraicky. Užívá při tom trigonometrické funkce úhlů velikosti $\frac{2\pi k}{p}$, kde $k = 1, 2, \dots, p-1$, které mohou být vyjádřeny jako kořeny určitých polynomů stupně p. Dochází k binomické rovnici $x^p - 1 = 0$ s kořeny ve tvaru $\cos\frac{2\pi k}{p} + i\sin\frac{2\pi k}{p}$, využívá tedy komplexní čísla a také primitivní kořeny modulo *n*. Větu, která určuje, kdy lze pravidelný *n*-úhelník eukleidovsky sestrojit dnes nazýváme podle jejího autora Gaussovou větou.

***Gaussova věta*:** Pravidelný *n*-úhelník je konstruovatelný pravítkem a kružítkem tehdy a jen tehdy, když $n = 2^r p_1 \dots p_s$, kde $r \geq 0$, $s \geq 0$, jsou celá čísla a $p_1, \dots, p_j$ jsou prvočísla ve tvaru $p_j = 2^{2^{r_j}} + 1$ pro kladné celé číslo r_j. (Stewart 2004, s. 218).

Čísla ve tvaru $p_j = 2^{2^{r_j}} + 1$ definoval v roce 1640 francouzský matematik *Pierre de Fermat* (1601–1665), když uvažoval, kdy je číslo ve tvaru $2^k + 1$ prvočíslem. Dokázal, že nutnou podmínkou je, aby k bylo mocninou čísla 2. Domníval se, že všechna čísla ve tvaru $F_n = 2^{2^n} + 1$ pro $n = 0, 1, 2, \dots$ jsou prvočísla. Čísla

$$F_0 = 2^{2^0} + 1 = 3$$
$$F_1 = 2^{2^1} + 1 = 5$$
$$F_2 = 2^{2^2} + 1 = 17$$
$$F_3 = 2^{2^3} + 1 = 257$$
$$F_4 = 2^{2^4} + 1 = 65\,537$$

jsou prvočísla, ale v r. 1732 švýcarský matematik *Leonhard Euler* (1707–1783) zjistil, že číslo $F_5 = 641 \cdot 6\,700\,417$ a tedy není prvočíslem (Stewart 2004, s. 219). Všechna čísla ve tvaru $F_n = 2^{2^n} + 1$ se tedy nazývají *Fermatova čísla*, pokud je F_n prvočíslo, říkáme, že je *Fermatovým prvočíslem* (Křížek 1995, s. 243).

Hledáním dalších složených Fermatových čísel se zabývala celá řada matematiků. V roce 1880 rozložil *F. Landry* F_6 na součin dvou činitelů[12], v roce 1897 ukázal *Felix Klein*, že F_7 je složené a v r. 1909 *J. C. Moreheard* a *A. E. Western* našli dělitele čísla F_8. Existují různé počítačové techniky, které hledají dělitele dalších čísel, otázka existence jiných Fermatových prvočísel je však dodnes otevřená, nikomu se doposud nepodařilo dokázat, že číslo F_4 je posledním Fermatovým prvočíslem. Stewart uvádí, že v době, kdy psal svoji knihu, bylo známo 210 Fermatových čísel, která jsou složená (Stewart 2004, s. 219). Do dnešní doby je podle Gaussovy věty počet eukleidovsky konstruovatelných pravidelných mnohoúhelníků s lichým počtem vrcholů $31 = 2^5 - 1$. (Křížek 1995, s. 244). Je zřejmé, že pokud uvažujeme i pravidelné mnohoúhelníky se sudým počtem vrcholů, je konstruovatelných pravidelných mnohoúhelníků nekonečně mnoho. Na konci své kapitoly VII Gauss uvádí výčet 38 čísel menších než 300 pro počet vrcholů sestrojitelných pravidelných mnohoúhelníků. Jsou to: 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272 (Gauss 1986, s. 478).

Nyní se vrátíme k samotné Gaussově větě. Své tvrzení shrnuje Gauss v bodě 465: „jestliže n je prvočíslo, redukovali jsme dělení kruhu na n částí na řešení takového počtu rovnic, jakého je počet dělitelů čísla $n-1$. Stupeň těchto rovnic je určen velikostí dělitelů. Proto kdykoli je $n-1$ mocninou čísla 2, což se stane, když je hodnota $n = 3,\ 5,\ 17,\ 257,\ 65\,537$, atd., je dělení kruhu omezeno pouze na kvadratické rovnice a goniometrické funkce úhlů $\frac{\pi}{n}, \frac{2\pi}{n}$, atd. pak mohou být vyjádřeny pomocí druhé odmocniny.“ (Gauss 1986, s. 476) Dále Gauss vyslovuje nutnou podmínku pro konstruovatelnost pravidelných mnohoúhelníků, kterou později dokázal Wantzel, jak jsme se již zmínili. Z Gaussových slov je ale patrné, že ví, jak by nutnost tvaru čísla n, dokázal, pouze se už jeho důkaz nevejde do už tak obsáhlého spisu. Bohužel důkaz nakonec nikdy nepublikoval. „Kdykoli $n-1$ obsahuje prvočíselné dělitele jiné než číslo 2, dovede nás to k rovnicím vyššího stupně, jmenovitě, k jedné nebo dvěma kubickým rovnicím, když se jednou nebo víckrát objeví mezi prvočíselnými děliteli čísla n číslo 3, k rovnicím 5. stupně, když $n-1$ je dělitelné 5, atd. Lze ukázat, že se těchto rovnic vyššího stupně žádným způsobem

[12] Již v roce 1855 píše Gaussovi německý astronom a matematik Thomas Clausen dopis, že číslo F_6 je složené. (Biermann 1964, s. 185)

nedokážeme zbavit, ani je zredukovat na rovnice nižších stupňů.“ (Gauss 1986, s. 477)

Při důkazu budeme sice vycházet z Gaussova řešení, abychom ale mohli dokázat zároveň nutnost i dostatečnost, podáme důkaz založený na Galoisově teorii. V roce 1824 dokázal norský matematik *Niels Abel* (1802–1829) neřešitelnost rovnice pátého stupně pomocí radikálů.[13] Francouzský matematik *Evariste Galois* (1811–1832) pak zobecnil Abelovy a Gaussovy metody, aby byl schopen zjistit, kdy má obecný polynom radikálové řešení. Nezávisle na sobě, zavedli Abel a Galois jazyk teorie grup, Galois pak použil tělesové rozšíření a grupy automorfismů.

V předložené práci ukážeme souvislost konstrukcí pravítkem a kružítkem s tělesovými rozšířeními. Definice tělesového rozšíření souvisí s polynomy a s hledáním jejich kořenů (zde vidíme souvislost s Gaussem). Pokud máme polynom nad nějakým tělesem K, které je podtělesem $\mathbb{C}$ a jeho kořeny neleží v tomto tělese, tak vezmeme nejmenší možné těleso L, které je podtělesem $\mathbb{C}$, přičemž $K \subset L$ a L obsahuje kořeny daného polynomu. Těleso L pak bude rozšířením původního tělesa.

2.3.2 Pomocné pojmy z Galoisovy teorie

Abychom mohli využívat Galoisovu teorii pro náš důkaz, musíme nejdříve zavést některé důležité pojmy. Vycházíme přitom z knihy *Galois Theory* (Stewart 2004). Omezíme se většinou na pouhý výčet jednotlivých definic a vět, jejichž důkazy jsou podány v již zmiňované knize. Cílem této podkapitoly není zavést Galoisovu teorii jako celek, nýbrž pouze ty části, které jsou nezbytné pro důkaz Gaussovy věty.

Definice 1: ***Tělesové rozšíření*** je monomorfismus $K \to L$, kde K, L jsou podtělesa tělesa komplexních čísel $\mathbb{C}$. Užíváme symbol $L : K$ pro rozšíření a říkáme, že L je rozšířením K.

Podle této definice je těleso reálných čísel rozšířením tělesa racionálních čísel, tedy $\mathbb{R} : \mathbb{Q}$ a těleso komplexních čísel je rozšířením tělesa reálných čísel, $\mathbb{C} : \mathbb{R}$. Nechť X je libovolnou podmnožinou $\mathbb{C}$, pak podtěleso tělesa $\mathbb{C}$ generované podmnožinou X, obsahuje $\mathbb{Q}$. Takové podtěleso značíme $\mathbb{Q}(X)$.

[13] Vycházel při tom z metod, které používal Joseph Louis Lagrange (1736–1813) a Gauss. Velkou zásluhu na tomto objevu má rovněž italský matematik Paolo Ruffini (1765–1822).

Definice 2: Jestliže $L : K$ je tělesovým rozšířením a Y je podmnožinou L, pak podtěleso tělesa $\mathbb{C}$ generované $K \cup Y$ se značí $K(Y)$ a říkáme, že vzniklo z K ***adjunkcí*** Y k tělesu K.

Pokud má Y pouze jeden prvek, $Y = \{\alpha\}$, hovoříme o ***jednoduchém rozšíření***. Místo označení $K(\{\alpha\})$ píšeme pouze $K(\alpha)$. Např. komplexní čísla jsou jednoduchým rozšířením reálných čísel, protože $Y = \{\mathrm{i}\}$, můžeme tedy napsat: $\mathbb{C} = \mathbb{R}(\mathrm{i})$. Podle toho, jaký je prvek α, může být jednoduché rozšíření buď *algebraické*, nebo *transcendentální*.

Definice 3: Nechť K je podtělesem $\mathbb{C}$ a nechť $\alpha \in \mathbb{C}$. Pak α je ***algebraické číslo*** nad K, jestliže existuje nenulový polynom p nad K takový, že $p(\alpha) = 0$. V opačném případě je α ***transcendentální*** nad K.

Například číslo $\alpha = \sqrt{3}$ je algebraické nad $\mathbb{Q}$, protože $\alpha^2 - 3 = 0$.

Definice 4: Nechť $K(\alpha) : K$ je jednoduché rozšíření. Pokud je α algebraický prvek nad K, nazýváme $K(\alpha) : K$ ***jednoduchým algebraickým rozšířením***, pokud je α transcendentální, nazýváme $K(\alpha) : K$ ***jednoduchým transcendentálním rozšířením***.

Definice 5: Říkáme, že tělesové rozšíření $L : K$ je ***algebraické rozšíření***, jestliže každý prvek z L je algebraický nad K.

Definice 6: Nechť $L : K$ je tělesové rozšíření a předpokládejme, že $\alpha \in L$ je algebraické číslo nad K. Pak ***minimálním polynomem*** prvku α nad K je jednoznačně daný normovaný polynom m nad K nejmenšího stupně takový, že $m(\alpha) = 0$.

Je-li α algebraický prvek, je možné chápat těleso $K(\alpha)$ jako vektorový prostor nad K. Dimenze tohoto prostoru je dána větou:

Věta 1: Nechť $K(\alpha) : K$ je jednoduché algebraické rozšíření a nechť m je minimální polynom α nad K a nechť $st(m) = n$. Pak $\{1, \alpha, \dots, \alpha^{n-1}\}$ je báze pro $K(\alpha)$ nad K. Dimenzí tělesa $K(\alpha)$ je počet prvků této báze.

Definice 7: Stupeň $[L : K]$ tělesového rozšíření $L : K$ je dimenze tělesa L, které uvažujeme jako vektorový prostor nad K.

L je vektorový prostor nad K, na prvky tělesa L se tedy můžeme dívat jako na vektory. Když vezmeme např. rozšíření $\mathbb{C} : \mathbb{R}$, $\mathbb{C}$ má dimenzi 2 nad $\mathbb{R}$, protože báze je $\{1, i\}$ a má 2 prvky, proto tedy stupeň $[\mathbb{C} : \mathbb{R}] = 2$.

Věta 2: Jestliže $K,\ L,\ M$ jsou podtělesa $\mathbb{C}$ a $K \subseteq L \subseteq M$, pak

$$[M : K] = [M : L] \cdot [L : K]$$

Důsledkem tohoto tvrzení je: Jestliže $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ jsou podtělesa $\mathbb{C}$, pak $[K_n : K_0] = [K_n : K_{n-1}] . [K_{n-1} : K_{n-2}] . \cdots . [K_1 : K_0]$.

Věta 3: Nechť $K(\alpha) : K$ je jednoduché rozšíření a nechť α je algebraické číslo. Pak $[K(\alpha) : K] = st(m)$, kde m je minimální polynom α nad K.

Např. Víme, že $\mathbb{C} = \mathbb{R}(i)$, kde i má minimální polynom $t^2 + 1$ stupně 2, takže $[\mathbb{C} : \mathbb{R}] = 2$, což souhlasí s naším předcházejícím výpočtem.

Definice 8: ***Konečné rozšíření*** je takové rozšíření, jehož stupeň je konečný.

Definice 9: Nechť $L : K$ je tělesové rozšíření. ***K-automorfismem*** L je automorfismus φ tělesa L takový, že $\varphi(k) = k$ pro všechna $k \in K$. Říkáme, že takové φ ***fixuje*** $k \in K$.

Věta 4: Jestliže je $L : K$ tělesové rozšíření, pak množina všech K-automorfismů L tvoří grupu s operací skládání zobrazení.

Definice 10: ***Galoisova grupa*** $\boldsymbol{\Gamma(L : K)}$ tělesového rozšíření $L : K$ je grupa všech K-automorfismů L s operací skládání zobrazení.

Dalším důležitým pojmem je Galoisova korespondence, což je vzájemně jednoznačné zobrazení mezi podgrupami Galoisovy grupy rozšíření $L : K$ a mezi podtělesy M tělesa L takovými, že $K \subseteq M$, přičemž toto zobrazení obrací inkluzivní relace. Nejdříve si popíšeme, jak vypadají podtělesa M.

Jestliže $L : K$ je rozšíření, ***mezitělesem*** nazýváme libovolné těleso M takové, že $K \subseteq M \subseteq L$. Pro rozšíření tedy platí, že L je rozšířením tělesa M, které je zároveň rozšířením tělesa K.

Každému mezitělesu M přiřadíme grupu $\boldsymbol{M^* = \Gamma(L : M)}$ všech M-automorfismů tělesa L. Takže K^* je celá Galoisova grupa $\Gamma(L : K)$ a $L^* = 1$. Pro libovolná mezitělesa rozšíření $L : K$ tedy platí, jestliže $M \subseteq N$, pak $M^* \supseteq N^*$.

Každé podgrupě H grupy $\Gamma(L:K)$ přiřadíme množinu $H^\dagger$ všech prvků $x \in L$ takových, že $\varphi(x) = x$ pro všechna $\varphi \in H$. Tato množina je mezitěleso. Pro H a $H^\dagger$ platí, že jestliže H je podgrupa Galoisovy grupy $\Gamma(L:K)$, pak $H^\dagger$ je podtělesem tělesa L obsahující K, tedy $K \subseteq H^\dagger$. $H^\dagger$ nazýváme ***fixním tělesem*** tělesa H. Zobrazení $\dagger$ také převrací inkluze, tedy jestliže $H \subseteq G$, pak $H^\dagger \supseteq G^\dagger$.

Jestliže M je mezitěleso a H je podgrupa Galoisovy grupy, pak

$$M \subseteq M^{*\dagger} \qquad (1)$$
$$H \subseteq H^{\dagger *}$$

Když označíme $\mathcal{F}$ množinu všech mezitěles rozšíření $L:K$ a $\mathcal{G}$ množinu všech podgrup Galoisovy grupy $\Gamma(L:K)$, pak definujeme dvě zobrazení:

$$*: \mathcal{F} \to \mathcal{G}$$
$$\dagger: \mathcal{G} \to \mathcal{F}$$

která převrací inkluze a splňují rovnice (1). Tato dvě zobrazení vytváří ***Galoisovu korespondenci*** mezi $\mathcal{F}$ a $\mathcal{G}$, jsou navzájem inverzní a vzájemně jednoznačná.

Př.: Polynom $f(t) = t^4 - 4t^2 - 5 = 0$ se rozkládá na $(t^2+1)(t^2-5) = 0$. Existují tedy 4 kořeny polynomu $f(t)$: $\alpha_1 = i,\ \alpha_2 = -i,\ \alpha_3 = \sqrt{5},\ \alpha_4 = -\sqrt{5}$. Přiřazené tělesové rozšíření je $\mathbb{Q}(i,\sqrt{5}) : \mathbb{Q}$, přičemž

$$\mathbb{Q}(i,\sqrt{5}) = \{p + qi + r\sqrt{5} + si\sqrt{5};\ p,q,r,s \in \mathbb{Q}\}$$

Stupeň tohoto rozšíření je 4, prvky $\{1, \sqrt{5},\ i,\ i\sqrt{5}\}$ tvoří bázi pro $\mathbb{Q}(i,\sqrt{5})$ nad $\mathbb{Q}$. Mezitělesa rozšíření $\mathbb{Q}(i,\sqrt{5}) : \mathbb{Q}$ jsou: $M_1 = \mathbb{Q}(i),\ M_2 = \mathbb{Q}(\sqrt{5}),\ M_3 = \mathbb{Q}(i\sqrt{5})$. Grupa všech $\mathbb{Q}$-automorfismů tělesa $\mathbb{Q}(i,\sqrt{5})$ obsahuje 4 prvky: $\{Id,\ \varphi_1,\ \varphi_2,\ \varphi_3\}$. Id je identita, $\varphi_1,\ \varphi_2,\ \varphi_3$ jsou cykly: $\varphi_1 = (\alpha_1\alpha_2),\ \varphi_2 = (\alpha_3\alpha_4),\ \varphi_3 = (\alpha_1\alpha_2)(\alpha_3\alpha_4)$.

automorfismy	i	$\sqrt{5}$
φ_1	$-i$	$\sqrt{5}$
φ_2	i	$-\sqrt{5}$
φ_3	$-i$	$\sqrt{5}$
Id	i	$\sqrt{5}$

Galoisova grupa $G = \{Id,\ \varphi_1,\ \varphi_2,\ \varphi_3\}$ $\mathbb{Q}$-automorfismů tělesa $\mathbb{Q}(i, \sqrt{5})$ obsahuje tyto podgrupy: $\{Id\},\ H_1 = \{Id, \varphi_1\},\ H_2 = \{Id, \varphi_2\},\ H_3 = \{Id, \varphi_3\}$.

Pokud vezmeme grupy G, H_1, H_2, H_3, $\{Id\}$, korespondující fixní tělesa k těmto grupám jsou po řadě $\mathbb{Q}$, M_1, M_2, M_3, $\mathbb{Q}(i, \sqrt{5})$. Vytvořili jsme tak Galoisovu korespondenci, která je bijekcí.

Následující definice nám přiblíží některé velmi důležité vlastnosti tělesových rozšíření, které souvisí s rozkladem polynomů na součin.

Definice 11: Jestliže K je podtělesem tělesa $\mathbb{C}$ a f je polynom nad K, pak f se ***rozkládá*** nad K, jestliže může být vyjádřen jako součin lineárních činitelů

$$f(t) = k(t - \alpha_1) \cdots (t - \alpha_n)$$

kde $k,\ \alpha_1, \ldots,\ \alpha_n \in K$.

Definice 12: Nechť Σ je podtělesem tělesa $\mathbb{C}$. Σ se nazývá ***rozkladové těleso*** polynomu f nad podtělesem K tělesa $\mathbb{C}$, jestliže $K \subseteq \Sigma$ a

1. f se rozkládá nad Σ
2. Jestliže $K \subseteq \Sigma' \subseteq \Sigma$ a f se dá rozložit nad Σ', pak $\Sigma' = \Sigma$.

Podmínku 2. bychom mohli napsat ještě jiným, ekvivalentním způsobem: $\Sigma = K(\alpha_1, \ldots, \alpha_n)$, kde $\alpha_1, \ldots, \alpha_n$ jsou kořeny polynomu f v Σ.

Věta 5: Jestliže K je libovolným podtělesem $\mathbb{C}$ a f je libovolný polynom nad K, pak existuje jednoznačné rozkladové těleso Σ pro f nad K. Stupeň $[\Sigma : K]$ je konečný.

Definice 13: Tělesové rozšíření $L : K$ je ***normální rozšíření***, jestliže každý ireducibilní polynom f nad K, který má v L alespoň jeden kořen, lze v L rozložit na součin lineárních činitelů.

Příkladem normálního rozšíření je $\mathbb{C} : \mathbb{R}$, protože každý polynom se rozkládá v $\mathbb{C}$. Na druhou stranu některá rozšíření nejsou normální, např. nechť α je reálná třetí odmocnina z čísla 2 a uvažujme rozšíření $\mathbb{Q}(\alpha) : \mathbb{Q}$. Ireducibilní polynom $t^3 - 2$ má kořen, je to α z $\mathbb{Q}(\alpha)$, ale nerozkládá se v $\mathbb{Q}(\alpha)$. Kdyby se rozkládal v $\mathbb{Q}(\alpha)$, existovaly by tři reálné různé třetí odmocniny z čísla 2, což není možné.

Věta 6: Tělesové rozšíření $L : K$ je normální a konečné tehdy a jen tehdy, když L je rozkladové těleso pro nějaký polynom nad K.

Následující věta nám ukáže, kdy je Galoisova grupa Abelova.

Věta 7: Nechť K je podtělesem $\mathbb{C}$, ve kterém se rozkládá polynom $t^n - 1$. Nechť $\alpha \in K$ a nechť L je rozkladové těleso pro $t^n - \alpha$ nad K. Pak Galoisova grupa rozšíření $L : K$ je Abelova.

Získané poznatky o Galoisově teorii nyní spojíme dohromady a vyslovíme její základní větu:

Věta 8 (Základní věta Galoisovy teorie): Jestliže $L : K$ je konečné, normální tělesové rozšíření v $\mathbb{C}$ s Galoisovou grupou G a jestliže $\mathcal{F}$, $\mathcal{G}$, $*$, $\dagger$ splňují podmínky, které jsme již definovali u Galoisovy korespondence, pak:

1. Galoisova grupa G má řád $[L : K]$.
2. Zobrazení $*$ a $\dagger$ jsou navzájem inverzní a tvoří vzájemně jednoznačnou korespondenci mezi $\mathcal{F}$ a $\mathcal{G}$, která převrací inkluze.
3. Jestliže M je mezitěleso, pak $[L : M] = |M^*|$ a $[M : K] = |G|/|M^*|$
4. Mezitěleso M je normálním rozšířením K tehdy a jen tehdy, když M^* je normální podgrupou G.
5. Jestliže mezitěleso M je normálním rozšířením K, pak Galoisova grupa rozšíření $M : K$ je izomorfní s faktorovou grupou G/M^*.

Další věta spojí dohromady stupeň tělesového rozšíření a řád grupy.

Věta 9: Nechť G je konečnou podgrupou grupy automorfismů tělesa K a nechť K_0 je fixní těleso grupy G. Pak $[K : K_0] = |G|$.

Důsledek: Jestliže G je Galoisova grupa konečného rozšíření $L : K$ a H je konečnou podgrupou G, pak $[H^\dagger : K] = [L : K]/|H|$.

V následujících řádcích si definujeme další důležitou vlastnost tělesových rozšíření, která souvisí s charakteristikou tělesa, nejdříve si tedy zavedeme tento pojem.

Definice 14: ***Základní*** podtěleso tělesa K je průnikem všech podtěles K.

Jinými slovy: základní těleso je takové těleso, které nemá žádné vlastní podtěleso.

Věta 10: Každé základní podtěleso je izomorfní buď s tělesem racionálních čísel $\mathbb{Q}$, nebo s tělesem $\mathbb{Z}_p$ zbytkových tříd celých čísel modulo prvočíslo p.

Definice 15: ***Charakteristika*** tělesa *K* je 0, jestliže základní podtěleso tělesa *K* je izomorfní s $\mathbb{Q}$, nebo je p, jestliže základní podtěleso *K* je izomorfní s $\mathbb{Z}_p$.

Z definice tedy vyplývá, že tělesa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ mají charakteristiku 0.

Definice 16: Ireducibilní polynom f nad tělesem *K* je ***separabilní*** nad *K*, jestliže nemá žádné násobné kořeny v rozkladovém tělese.

Příklad: Uvažujme polynom $f(t) = t^2 + t + 1$ nad $\mathbb{Z}_2$. Těleso $\mathbb{Z}_2$ je tělesem zbytkových tříd celých čísel modulo 2 a má 2 prvky, 0 a 1. Víme, že polynom f je ireducibilní, takže můžeme připojit prvek ξ takový, že ξ má minimální polynom f nad $\mathbb{Z}_2$. Pak $\xi^2 + \xi + 1 = 0$, takže $\xi^2 = 1 + \xi$, těleso $\mathbb{Z}_2$ má charakteristiku 2. Prvky 0, 1, ξ, $1 + \xi$ tvoří těleso, vycházíme ze součtové a multiplikační tabulky:

$+$	0	1	ξ	$1+\xi$
0	0	1	ξ	$1+\xi$
1	1	0	$1+\xi$	ξ
ξ	ξ	$1+\xi$	0	1
$1+\xi$	$1+\xi$	ξ	1	0

.	0	1	ξ	$1+\xi$
0	0	0	0	0
1	0	1	ξ	$1+\xi$
ξ	0	ξ	$1+\xi$	1
$1+\xi$	0	$1+\xi$	1	ξ

Při výpočtech v multiplikační tabulce jsme postupovali takto:

$$\xi(1+\xi) = \xi + \xi^2 = \xi + \xi + 1 = 1$$

Tudíž $\mathbb{Z}_2(\xi)$ je těleso se čtyřmi prvky. Nyní se f rozkládá nad $\mathbb{Z}_2(\xi)$:

$$t^2 + t + 1 = (t - \xi)(t - 1 - \xi)$$

Ale nerozkládá se nad žádnými menšími tělesy, proto $\mathbb{Z}_2(\xi)$ je rozkladové těleso pro f nad $\mathbb{Z}_2$. Polynom f je separabilní nad $\mathbb{Z}_2$.

Věta 11: Jestliže K je těleso charakteristiky 0, pak každý ireducibilní polynom nad K je separabilní nad K. Jestliže K má charakteristiku $p > 0$, pak ireducibilní polynom f nad K je neseparabilní tehdy a jen tehdy, když $f(t) = k_0 + k_1 t^p + \cdots + k_r t^{rp}$, kde $k_0, \ldots, k_r \in K$.

Definice 17: Libovolný polynom nad K je *separabilní* nad K, jestliže všechny jeho ireducibilní činitelé jsou separabilní nad K. Jestliže $L : K$ je rozšíření, pak algebraický prvek $\alpha \in L$ je *separabilní* nad K, jestliže minimální polynom nad K je separabilní nad K. Algebraické rozšíření $L : K$ je *separabilním* rozšířením, jestliže každé $\alpha \in L$ je separabilní nad K.

Číselným tělesem budeme nazývat podtěleso komplexních čísel, jež je zároveň algebraickým rozšířením tělesa $\mathbb{Q}$, které má konečný stupeň. Protože každé algebraické rozšíření $\mathbb{Q}$ je separabilní ($\mathbb{Q}$ má charakteristiku 0), mají číselná tělesa tento tvar: $K = \mathbb{Q}(\alpha)$, kde $\alpha \in \mathbb{C}$ je nějaký algebraický prvek nad $\mathbb{Q}$.

Definice 18: Prvky a a b z grupy G jsou ***konjugované*** v G, jestliže v G existuje takový prvek g, že $a = g^{-1}bg$.

Konjugace je ekvivalence, třídy ekvivalence této relace se nazývají *konjugované třídy* v G, označíme je $C_1, \ldots, C_r$. Platí tzv. *rovnice tříd G:* $|G| = 1 + |C_2| + \cdots + |C_r|$, $|C_1| = 1$ (identita). $|G|$ je označení pro řád grupy (počet jejích prvků).

Věta 12: Počet prvků libovolné konjugované třídy konečné grupy G dělí řád grupy G.

Definice 19: ***Centrum $Z(G)$*** grupy G je množina všech prvků $x \in G$ takových, že $xg = gx$ pro všechna $g \in G$.

$Z(G)$ je tedy podgrupou grupy G, každý její člen komutuje s libovolným členem grupy. Pro Abelovu grupu platí $Z(G) = G$.

Věta 13: Jestliže A je konečná Abelova grupa, jejíž řád je dělitelný prvočíslem p, pak A má prvek řádu p.

2.3.3 Konstruovatelnost kružítkem a pravítkem z hlediska algebry

Abychom dokázali převést geometrický problém na algebraické vyjádření, musíme si uvědomit, že jakákoli geometrická konstrukce se dá přeformulovat do tvaru, kde je zadaná určitá množina prvků $a, b, c, \ldots$ a jeden nebo více prvků $x, y, \ldots$, které hledáme. Požadovanými prvky může být například poloměr kružnice, střed úsečky, strana

pravidelného mnohoúhelníku. Geometrická konstrukce se pak rovná řešení algebraického problému: nejdříve musíme najít vztah (vyjádřený nějakou rovnicí) mezi požadovanou veličinou x a danými veličinami $a, b, c, \dots$, poté je nutné najít neznámou veličinu x vyřešením této rovnice a nakonec je třeba určit, zda jsme schopni dosáhnout výsledku pomocí operací, které odpovídají konstrukci pravítkem a kružítkem (tedy, jak již bylo napsáno v kap. 1 pomocí součtu, rozdílu, součinu, podílu a druhé odmocniny). (Courant 1996, s. 120)

Pro důkaz věty o konstruovatelnosti pravidelných mnohoúhelníků budeme využívat *algebraickou formulaci* konstruovatelnosti kružítkem a pravítkem podle knihy *Galois Theory* (Stewart 2004, s. 76–79), kterou si nyní přiblížíme, přičemž pravítko nám slouží ke spojování dvou bodů, nikoli k měření délek, pro zavedení nějaké dané délky velikosti 1 nám slouží kružítko.

Nejprve si zavedeme pojem ***konstruovatelný bod***.

Nechť je dána množina bodů P v rovině $\mathbb{R}^2$, pak zavedeme dvě následující operace:
Pravítko: Dvěma různými body z P sestrojit přímku.
Kružítko: Sestrojit kružnici, jejíž střed je bod z P a poloměr je vzdálenost dvou libovolných bodů z P.

Definice 20: Říkáme, že bod vzniklý jako průsečík dvou různých přímek nebo kružnic za použití operací pravítka a kružítka je ***konstruovatelný jedním krokem*** z množiny P. Bod $A \in \mathbb{R}^2$ je ***konstruovatelný*** z P, jestliže existuje konečný počet $A_1, \dots, A_n = A$ bodů z $\mathbb{R}^2$ takových, že pro každé $j = 1, \dots, n$ je bod A_j konstruovatelný jedním krokem z množiny $P \cup \{A_1, \dots, A_{j-1}\}$.

Takto zavedené konstrukce kružítkem a pravítkem nyní položíme do vztahu s tělesovým rozšířením. Každému úseku konstrukce přičleníme podtěleso tělesa $\mathbb{C}$ generované souřadnicemi sestrojených bodů, které je zároveň i podtělesem $\mathbb{R}$. Tedy nechť K_0 je podtělesem $\mathbb{R}$ generované souřadnicemi bodů z P. Jestliže A_j má souřadnice (x_j, y_j), pak induktivně definujeme K_j jako těleso získané z K_{j-1} přidáním x_j, y_j, takže $K_j = K_{j-1}(x_j, y_j)$. Tímto způsobem vznikne řada podtěles

$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$$

tuto řadu použijeme pro odvození kritéria konstruovatelnosti.

Věta 14: Podle popisu výše jsou x_j, y_j kořeny v K_j kvadratického polynomu nad K_{j-1}.

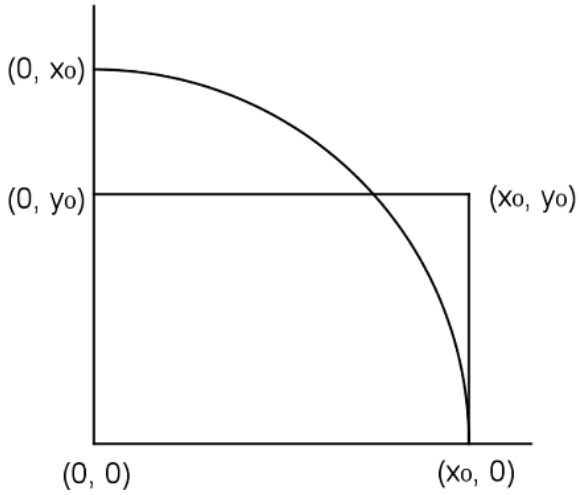
Důkaz této věty je v (Stewart 2004, s. 78).

Věta 15: Jestliže $A = (x, y)$ je konstruovatelný jedním krokem z $P \subseteq \mathbb{R}^2$ a K_0 je podtělesem $\mathbb{R}$ generované souřadnicemi bodů z *P*, pak

$$[K_0(x) : K_0] = [K_0(y) : K_0] = 2$$

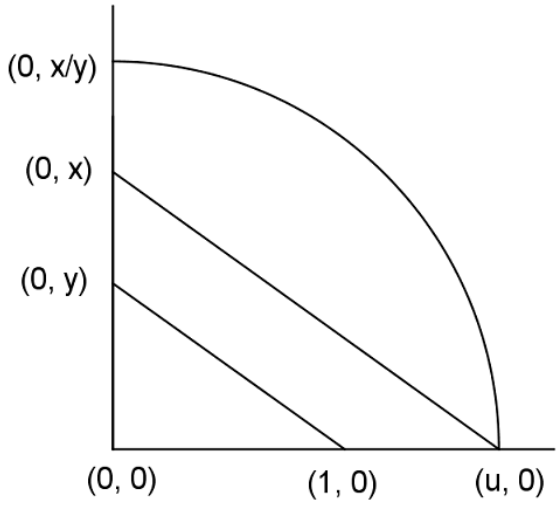
Důkaz: Použitím věty 14 a důsledku věty 2 je $[K_j : K_{j-1}] = 2$, $[K_n : K_0] = 2$. Ale protože $[K_n : K_0(x)] \cdot [K_0(x) : K_0] = [K_n : K_0]$ a $[K_n : K_0(x)] = 1$, musí být $[K_0(x) : K_0] = 2$. Důkaz $[K_0(y) : K_0] = 2$ je analogický.

Věta 16: Nechť *P* je podmnožina kartézského součinu $\mathbb{R}^2$, která obsahuje body (0, 0) a (1, 0). Pak bod (x, y) je *konstruovatelný* z *P*, jestliže x a y leží v podtělese $\mathbb{R}$, které je generované souřadnicemi bodů z *P*.



Obr. 1: Konstrukce bodů $(0, x_0)$, $(0, y_0)$ *z* (x_0, y_0)

Důkaz: Pokud máme daný libovolný bod (x_0, y_0) a chceme z něj získat body $(0, x_0)$ a $(0, y_0)$, nejdříve sestrojíme z bodů (0, 0) a (1, 0) souřadnicové osy a pak budeme postupovat podle obr. 1.



Obr. 2: Konstrukce bodu $\left(0, \frac{x}{y}\right)$

Naopak, jestliže máme dány body $(0, x_0)$, $(0, y_0)$, pak nám stejná konstrukce, ale v obráceném pořadí dá bod (x_0, y_0). Stačí nám tedy dokázat, že z daných bodů $(0, x)$, $(0, y)$ jsme schopni sestrojit body $(0, x + y)$, $(0, x - y)$, $(0, xy)$, $\left(0, \frac{x}{y}\right)$, když $y \neq 0$. Pro sestrojení prvních dvou bodů opíšeme oblouk se středem v $(0, x)$ a poloměrem y, který nám protne osu y v bodech $(0, x + y)$, $(0, x - y)$. Další dva body získáme následovně: spojíme bod (1, 0) s bodem $(0, y)$ a sestrojíme rovnoběžku s touto spojnicí procházející bodem

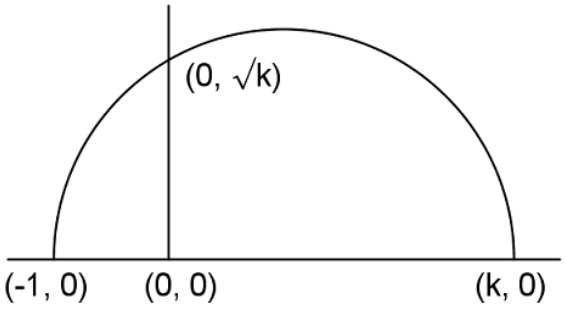
$(0,\ x)$. Tato přímka nám protne osu x v bodě $(u,\ 0)$. Díky podobnosti získaných trojúhelníků dostaneme vztah $\frac{u}{x} = \frac{1}{u}$, z toho vyplývá $u = \frac{x}{y}$, sestrojili jsme tedy bod $\left(\frac{x}{y},\ 0\right)$ a tedy i bod $\left(0,\ \frac{x}{y}\right)$, obr. 2. Když vezmeme $x = 1$, můžeme sestrojit bod $\left(\frac{1}{y},\ 0\right)$ a díky tomu i bod $\left(0,\ \frac{1}{y}\right)$, který se nám hodí pro konstrukci posledního bodu. Když totiž vezmeme $\frac{1}{y}$ místo y, dostaneme bod $(xy,\ 0)$, z něj už pak snadno získáme hledaný bod $(0,\ xy)$.

Věta 17: Nechť $K(\alpha) : K$ je rozšíření stupně 2 takové, že $K(\alpha) \subseteq \mathbb{R}$. Pak libovolný bod $(u,\ v)$ z $\mathbb{R}^2$, jehož souřadnice leží v $K(\alpha)$ může být sestrojen z nějaké vhodné konečné množiny bodů, jejichž souřadnice leží v K.

Důkaz: Předpokládáme, že $[K(\alpha) : K] = 2$, pak podle věty 3 je $st(m) = 2$ a tedy minimální polynom m má tvar $\alpha^2 + p\alpha + q = 0,\ p,\ q \in K$. Takže

$$\alpha = \frac{-p \pm \sqrt{p^2 - 4q}}{2}$$

Protože $K(\alpha) \subseteq \mathbb{R}$, musí být $p^2 - 4q$ kladné. Použitím definice 20 již získáme výsledek, jestliže umíme sestrojit $\left(0, \sqrt{k}\right)$ pro libovolné kladné $k \in K$ z konečného počtu bodů $(x_r,\ y_r)$, kde $x_r,\ y_r \in K$. Sestrojíme tedy body (-1, 0) a (k, 0). Narýsujeme půlkružnici nad průměrem z těchto bodů, ta nám protne osu y v bodě (0, v). Podle Euklidovy věty o výšce platí $v^2 = 1 \cdot k$, takže $v = \sqrt{k}$, obr. 3.



Obr. 3: Konstrukce bodu $\left(0, \sqrt{k}\right)$

Věta 18: Nechť K je podtělesem $\mathbb{R}$ generovaným souřadnicemi bodů z $P \subseteq \mathbb{R}^2$. Nechť $\alpha,\ \beta$ leží v rozšíření L tělesa K a je obsaženo v $\mathbb{R}$ tak, že existuje konečná řada podtěles

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L$$

takových, že $[K_{j+1} : K_j] = 2$ pro $j = 0, \ldots, r-1$. Pak bod $(\alpha,\ \beta)$ je konstruovatelný z P.

Důkaz: Pokud $r = 0$, pravdivost tvrzení vyplývá přímo z věty 16, pokud $r \neq 0$, bod (α, β) podle věty 17 je konstruovatelný z konečného počtu bodů, jejichž souřadnice leží v K_{r-1}. Jednotlivé body jsou konstruovatelné z P, takže i bod (α, β) je konstruovatelný z P. Blíže viz (Stewart 2004, s. 214).

Věta 19: Jestliže G je konečná grupa a $|G| = 2^r$, pak $Z(G)$ obsahuje prvek řádu 2.

Důkaz: Podle tzv. *rovnice tříd* grupy G platí: $1 + |C_2| + \cdots + |C_k| = 2^r$. Aby platila rovnost, musí být nějaké C_j liché, podle věty 12 počet prvků C_j dělí 2^r, tedy musí být $|C_j| = 1$ a z toho plyne, že $Z(G) \neq 1$. Dále použijeme větu 13. $Z(G)$ je konečná Abelova grupa, její řád nemůže být větší než 2^r, musí být tedy dělitelný prvočíslem 2 a podle zmíněné věty má $Z(G)$ prvek řádu 2.

Důsledek 1: Jestliže G je konečná grupa a $|G| = 2^r$, pak existuje řada normálních podgrup $1 = G_0 \subseteq \cdots \subseteq G_r = G$ takových, že $|G_j| = 2^j$ pro $0 \leq j \leq r$.

Důkaz: Vyplývá z věty 19 a indukce.

Věta 20: Jestliže K je podtělesem $\mathbb{R}$ generované souřadnicemi bodů z $P \subseteq \mathbb{R}^2$ a jestliže α a β leží v normálním rozšíření $L : K$ takovém, že $L \subseteq \mathbb{R}$ a $[L : K] = 2^r$ pro nějaké celé číslo r, pak (α, β) je konstruovatelný z P.

Důkaz: Protože má těleso charakteristiku 0 (je podtělesem $\mathbb{R}$), rozšíření $L : K$ je separabilní. Vezmeme grupu G takovou, že je Galoisovou grupou rozšíření $L : K$. Podle bodu 1. věty 8 má tato grupa stejný řád jako rozšíření, tedy $|G| = 2^r$. Pak ale podle důsledku 1 existuje řada normálních podgrup $1 = G_0 \subseteq \cdots \subseteq G_r = G$ takových, že $|G_j| = 2^j$ pro $0 \leq j \leq r$. Nechť dále K_j je fixní těleso grupy $G_{r-j}^{\dagger}$. Potom podle bodu 3. věty 8 je $[K_{j+1} : K_j] = 2$ pro všechna j. Konečně podle věty 18 je bod (α, β) z P.

2.3.4 Konstruovatelnost pravidelných mnohoúhelníků

V tuto chvíli už máme připravené téměř všechny důležité pojmy, abychom mohli dokázat Gaussovu větu. Vyslovíme ještě poslední definici, která nám říká, kdy je konstruovatelné nějaké číslo. Dále budeme opět postupovat podle knihy (Stewart 2004).

Definice 21: Kladné celé číslo n je ***konstruovatelné***, jestliže je pravidelný n-úhelník konstruovatelný pomocí pravítka a kružítka.

Nyní již přistoupíme k samotnému důkazu, prvním úkolem bude zredukovat problém na takové hodnoty n, které jsou prvočísla.

Věta 21: Jestliže je n konstruovatelné a m dělí n, pak m je také konstruovatelné. Jestliže jsou n a m nesoudělná a konstruovatelná čísla, pak součin mn je konstruovatelný.

Důkaz: Jestliže m dělí n, pak jsme schopni sestrojit pravidelný m-úhelník tak, že spojíme každý d-tý vrchol pravidelného n-úhelníku, kde $d = \frac{n}{m}$. Jestliže m a n jsou nesoudělná, pak existují $a, b \in \mathbb{Z}$ taková, že $am + bn = 1$. Pokud tuto rovnici vydělíme součinem mn (můžeme si to dovolit, předpokládáme, že obě čísla jsou nenulová), dostaneme vztah

$$\frac{1}{mn} = \frac{a}{n} + \frac{b}{m}$$

Proto z úhlů $\frac{2\pi}{m}$ a $\frac{2\pi}{n}$ můžeme sestrojit $\frac{2\pi}{mn}$ a z tohoto úhlu už získáme pravidelný mn-úhelník jednoduše.

Důsledek 2: Předpokládejme, že $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, kde $p_1, \dots, p_r$ jsou navzájem různá prvočísla. Pak n je konstruovatelné tehdy a jen tehdy, když každé $p_j^{\alpha_j}$ je konstruovatelné.

Důkaz: Vyplývá přímo z věty 21.

Věta 22: Pro každé kladné celé číslo α je číslo 2^{α} konstruovatelné.

Důkaz: Každý úhel umíme rozpůlit pomocí kružítka a pravítka, na tento výsledek pak aplikujeme indukci (můžeme úhel půlit znovu a znovu, dokud nedostaneme požadovaný výsledek).

Tímto omezujeme konstruovatelnost pravidelných mnohoúhelníků na případ, kdy je počet stran mnohoúhelníku, tedy číslo n, liché prvočíslo. Pokud se přesuneme do algebry, víme, že v komplexní rovině tvoří vrcholy pravidelného n-úhelníku množina n-tých odmocnin z jedničky. Tyto odmocniny jsou kořeny v $\mathbb{C}$ polynomu

$$t^n - 1 = (t - 1)(t^{n-1} + t^{n-2} + \dots + t + 1)$$

Dále se zaměříme na polynom $(t^{n-1} + t^{n-2} + \dots + t + 1)$.

Věta 23: Nechť p je prvočíslo takové, že p^n je konstruovatelné. Nechť ξ je primitivní p^n-tá odmocnina z jedničky v $\mathbb{C}$, přičemž primitivní p-tá odmocnina z jedničky má tvar

$$\xi_p = \cos\frac{2\pi}{p} + \sin\frac{2\pi}{p}$$

Pak stupeň minimálního polynomu ξ nad $\mathbb{Q}$ je mocnina čísla 2.

Důkaz: Nechť $\xi = \cos\frac{2\pi}{p^n} + \sin\frac{2\pi}{p^n}$. Protože p^n je konstruovatelné, můžeme sestrojit promítnutím vrcholu pravidelného p-úhelníku na souřadnicové osy bod (α, β) takový, že $\alpha = \cos(2\pi/p^n)$ a $\beta = \sin(2\pi/p^n)$. Podle věty 18 je

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 2^r$$

pro nějaké celé číslo r. Odtud snadno dostaneme tvar

$$[\mathbb{Q}(\alpha, \beta, i) : \mathbb{Q}] = 2^r . 2 = 2^{r+1}$$

Ale těleso $\mathbb{Q}(\alpha, \beta, i)$ obsahuje $\alpha + i\beta = \xi$, takže $[\mathbb{Q}(\xi) : \mathbb{Q}]$ musí být mocnina 2, protože $\mathbb{Q}(\xi) \subseteq \mathbb{Q}(\alpha, \beta, i)$. Tímto jsme dokázali, že stupeň minimálního polynomu prvku ξ je mocnina čísla 2. Dále bychom měli vypočítat příslušné minimální polynomy, abychom našli jejich stupeň, bude stačit, když vezmeme p a p^2.

Věta 24: Jestliže p je prvočíslo a ξ je primitivní p-tá odmocnina z jedničky v $\mathbb{C}$, pak minimální polynom z ξ nad $\mathbb{Q}$ je $f(t) = 1 + t + \cdots + t^{p-1}$.

Důkaz: Jak jsme již poznamenali, je

$$f(t) = \frac{t^p - 1}{t - 1}$$

Dále víme, že $f(\xi) = 0$, jelikož $\xi^p - 1 = 0$ a $\xi \neq 1$. Důkaz bude hotov, pokud ukážeme, že polynom $f(t)$ je ireducibilní. Zavedeme substituci $u = t - 1$, tedy $t = 1 + u$. Pak $f(t)$ je ireducibilní nad $\mathbb{Q}$ právě tehdy, když $f(1 + u)$ je ireducibilní. Polynom

$$f(1 + u) = \frac{(1 + u)^p - 1}{u} = u^{p-1} + ph(u)$$

kde h je polynom v proměnné u nad $\mathbb{Z}$ s konstantním členem 1 (vycházíme z toho, co známe o binomických koeficientech). Podle Eisensteinova kritéria[14] je $f(1+u)$ ireducibilní nad $\mathbb{Q}$, tedy i polynom $f(t)$ je ireducibilní nad $\mathbb{Q}$.

Věta 25: Jestliže p je prvočíslo a ξ je primitivní p^2-tá odmocnina jedničky v $\mathbb{C}$, pak minimální polynom z ξ nad $\mathbb{Q}$ je $g(t) = 1 + t^p + \cdots + t^{p(p-1)}$.

Důkaz: Jako ve větě 24 vycházíme z toho, že polynom $g(t)$ jsme získali z polynomu $t^{p^2} - 1$, můžeme ho tedy zapsat ve tvaru

$$g(t) = \frac{t^{p^2} - 1}{t^p - 1}$$

Nyní $\xi^{p^2} - 1 = 0$, ale $\xi^p - 1 \neq 0$, takže musí být $g(\xi) = 0$. Dále stačí ukázat, že polynom $g(t)$ je ireducibilní nad $\mathbb{Q}$. Když nejdříve, jako v předešlém důkazu, zavedeme substituci $t = 1 + u$, pak

$$g(1+u) = \frac{(1+u)^{p^2} - 1}{(1+u)^p - 1}$$

Když vezmeme modulo p, dostaneme

$$\frac{(1+u)^{p^2} - 1}{(1+u)^p - 1} \equiv u^{p(p-1)} \pmod{p}$$

Tedy $g(1+u) = u^{p(p-1)} + pk(u)$, kde $k(u)$ je polynom v proměnné u nad $\mathbb{Z}$. Ze vztahu $g(1+u) = 1 + (1+u)^p + \cdots + (1+u)^{p(p-1)}$ vyplývá, že $k(u)$ má konstantní člen 1. Z Eisensteinova kritéria nám opět vyplývá, že polynom $g(1+u)$ a tudíž i polynom $g(t)$ je ireducibilní.

Nyní můžeme konečně přistoupit na důkaz Gaussovy věty, nejdříve si však připomeneme její znění:

Gaussova věta: „Pravidelný n-úhelník je konstruovatelný pravítkem a kružítkem tehdy a jen tehdy, když $n = 2^r p_1 \dots p_s$, kde $r \geq 0$, $s \geq 0$, jsou celá čísla a $p_1, \dots, p_j$ jsou lichá prvočísla ve tvaru $p_j = 2^{2^{r_j}} + 1$ pro kladné celé číslo r_j." (Stewart, s. 218).

[14] Eisensteinovo kritérium: Nechť $f(t) = a_0 + a_1 + \cdots + a_n t^n$ je polynom nad $\mathbb{Z}$. Předpokládejme, že existuje prvočíslo q takové, že splňuje podmínky, viz níže. Pak řekneme, že f je ireducibilní nad $\mathbb{Q}$.

1. $q \nmid a_n$
2. $q \mid a_i \ (i = 0, \dots, n-1)$
3. $q^2 \nmid a_0$ (Stewart 2004, s. 40).

Důkaz: Nechť n je konstruovatelné číslo. Pak $n = 2^r p_1^{\alpha_1} \dots p_s^{\alpha_s}$, kde $p_1 \dots p_s$ jsou různá lichá prvočísla. Podle důsledku 2 je každé $p_j^{\alpha_j}$ konstruovatelné. Jestliže je $\alpha_j \geq 2$ pak podle věty 18 je p_j^2 konstruovatelné. Proto je stupeň minimálního polynomu primitivní p_j^2-té odmocniny z jedničky nad $\mathbb{Q}$ podle věty 23 roven mocnině čísla 2. Dále pak podle věty 25 je $p_j(p_j - 1)$ mocninou 2, to je ale spor s předpokladem, protože p_j je liché. Proto musí platit, že $\alpha_j = 1$ pro všechna j. Číslo p_j je tedy konstruovatelné. Podle věty 24 platí, že $p_j - 1 = 2^{s_j}$ pro nějaké vhodné s_j. Předpokládejme, že s_j má lichého dělitele $a > 1$, takže $s_j = ab$. Pak

$$p_j = (2^b)^a + 1$$

To je ale dělitelné číslem ve tvaru $2^b + 1$, protože platí

$$t^a + 1 = (t + 1)(t^{a-1} - t^{a-2} + \cdots + 1)$$

když a je liché. V tom případě ale p_j nemůže být prvočíslo, což je opět spor s předpokladem. Proto číslo s_j nesmí mít liché dělitele, takže je ve tvaru $s_j = 2^{r_j}$ pro nějaké $r_j > 0$. Takto jsme dokázali nutnou podmínku pro tvar čísla n, ještě musíme dokázat podmínku dostačující. Podle důsledku 2 můžeme uvažovat pouze takové dělitele čísla n, které jsou mocniny prvočísel. Podle věty 22 je číslo 2^r konstruovatelné. Musíme tedy dokázat, že každé p_j je také konstruovatelné. Nechť ξ je primitivní p-tá odmocnina z jedničky. Pak $[\mathbb{Q}(\xi) : \mathbb{Q}] = p_j - 1 = 2^a$ pro nějaké a, vycházíme při tom z věty 23. $\mathbb{Q}(\xi)$ je nyní rozkladové těleso pro polynom

$$f(t) = 1 + t + \cdots + t^{p-1}$$

nad $\mathbb{Q}$, takže tělesové rozšíření $\mathbb{Q}(\xi) : \mathbb{Q}$ je normální, zároveň je však také separabilní, protože $\mathbb{Q}$ má charakteristiku 0. Podle věty 7 je Galoisova grupa $\Gamma(\mathbb{Q}(\xi) : \mathbb{Q})$ Abelova. Vezmeme těleso K takové, že $K = \mathbb{R} \cap \mathbb{Q}(\xi)$. Pak

$$\cos\frac{2\pi}{p_j} = \frac{\xi + \xi^{-1}}{2} \in K$$

Tělesové rozšíření $\mathbb{Q}(\xi) : K$ má stupeň 2, takže $\Gamma(\mathbb{Q}(\xi) : K)$ je podgrupou grupy $G = \Gamma(\mathbb{Q}(\xi) : \mathbb{Q})$ řádu 2, vycházíme při tom z věty 8. Dokonce je normální podgrupou, protože G je Abelova grupa. Tudíž $K : \mathbb{Q}$ je normální rozšíření stupně

2^{a-1}. Podle věty 20 je bod $\left(\cos\frac{2\pi}{p_j},\ 0\right)$ konstruovatelný. Z tohoto důvodu je i číslo p_j konstruovatelné, čímž je dostatečnost dokázána a důkaz je kompletní.

3 Konstrukce pravidelného sedmnáctiúhelníku

V dopise ze dne 6. ledna 1819, který psal Gauss Christianu Ludwigu Gerlingovi (1788–1864), rozvádí myšlenku zavedení teorie mnohoúhelníků přes mnohoúhelník o 17 stranách a píše: „Ačkoli ode mě do dnešní doby nebyla publikována nikde žádná zmínka o historii tohoto objevu, mohu ji podat naprosto přesně. Bylo to 29. března 1796[15] a náhoda s tím rozhodně neměla nic společného. Skutečně, před tím, během zimy 1796 (můj první semestr v Göttingenu) jsem již objevil všechno, co souviselo se separací kořenů rovnice $\frac{x^p-1}{x-1}=0$ do dvou grup […]. Po usilovných úvahách o vzájemném vztahu všech kořenů, postaveném na aritmetických základech, se mi podařilo během prázdnin v Brunšviku, ráno v již zmiňovaný den (před tím, než jsem musel vstát z postele), najít tento vztah tím nejzřejmějším způsobem, takže jsem mohl okamžitě vytvořit speciální aplikaci pro 17-úhelník a pro číselné aplikace.“ (Archibald 1920, s. 324)

V této kapitole si nejdříve předvedeme konstrukci pravidelného 17-úhelníku podle Gausse, tedy jeho teoretický výpočet, neboť samotnou geometrickou konstrukci Gauss nikdy nevydal. Budeme při tom vycházet z (Gauss, 1986) a (Stewart 2004). Poté si popíšeme některé další známé konstrukce.

3.1.1 Gaussův teoretický výpočet

Z výsledků předešlé kapitoly víme, že pokud máme sestrojit pravidelný mnohoúhelník o n stranách, musíme najít kořeny rovnice $t^n-1=0$. Tyto kořeny pak budou představovat n vrcholů pravidelného mnohoúhelníku, které budou ležet na jednotkové kružnici se středem v bodě (0, 0). Protože jedním z kořenů této rovnice je $\varepsilon_0=1$, bude mít jeden z vrcholů pravidelného n-úhelníku souřadnice (1, 0). Původní rovnici pak můžeme upravit takto:

$$\frac{t^n-1}{t-1}=t^{n-1}+t^{n-2}+\cdots+t+1$$

Dále nás tedy bude zajímat rovnice

$$t^{n-1}+t^{n-2}+\cdots+t+1=0 \qquad (1)$$

Kořeny rovnice (1) označíme $\varepsilon_1,\ \varepsilon_2,\ldots,\ \varepsilon_{n-1}$, které podle Moivreovy věty lze zapsat do tvaru

[15] Všeobecně je znám datum 30. března 1796, např. (Tietze 1965, s. 182)

$$\varepsilon_k = \cos k\theta + i \sin k\theta\,, \qquad \theta = \frac{2\pi}{n}, \qquad k = 1, 2, \dots, n$$

Zároveň pro jednotlivé kořeny platí, že číslo označení v indexu je stejné jako exponent kořene ε_1, tedy $\varepsilon_1 = \varepsilon_1^1 = \varepsilon, \varepsilon_2 = \varepsilon_1^2 = \varepsilon^2, \dots, \varepsilon_{n-1} = \varepsilon_1^{n-1} = \varepsilon^{n-1}$ a pro libovolné k je $\varepsilon_k^n = 1$.

Dalším důležitým vztahem mezi kořeny rovnice (1) je:

$$\varepsilon + \varepsilon_2 + \cdots + \varepsilon_{n-1} = -1 \qquad (2)$$

Nyní si přiblížíme ***Gaussův teoretický výpočet***. Nechť Ω je množina všech kořenů rovnice (1), Gauss píše[16]: „Ω se bude shodovat s prvky ε^e, $\varepsilon^{2e}, \dots$, $\varepsilon^{(n-1)e}$, kde e je libovolné kladné nebo záporné celé číslo takové, že není dělitelné číslem n. Rovnici (1) pak můžeme napsat ve tvaru $(t - \varepsilon^e)(t - \varepsilon^{2e}) \dots \left(t - \varepsilon^{(n-1)e}\right) = 0$.“ (Gauss 1986, str. 411). Pro zjednodušení používá pro ε^λ značení $[\lambda]$ pro každé celé číslo λ. Dále uvádí: „Pro libovolná celá čísla λ, μ platí $[\lambda] = [\mu]$ právě tehdy, když λ a μ jsou kongruentní vzhledem k modulo n. […] takže $[0] = 1$; $[\lambda] \cdot [\mu] = [\lambda + \mu]$; $[\lambda]^\nu = [\lambda\nu]$. Součet $[0] + [\lambda] + [2\lambda] + \cdots + [(n-1)\lambda]$ je buď 0, nebo n podle toho, zda je λ dělitelné číslem n nebo není.“ (Gauss 1986, s. 414)

Dále používá pojem primitivní kořen, který zavedl již v kapitole III: g je ***primitivním kořenem*** čísla n, jestliže mocniny g, g^2, $g^3, \dots$ modulo n představují všechna čísla $1, 2, \dots, n-1$. „Nechť g je primitivním kořenem n, pak čísla $1, g, g^2, \dots, g^{n-2}$ budou kongruentní číslům $1, 2, 3, \dots, n-1$ vzhledem k modulo n. Takže kořeny $[1], [g], \dots, [g^{n-2}]$ se shodují s prvky Ω a ze stejného důvodu i kořeny $[\lambda], [\lambda g], \dots, [\lambda g^{n-2}]$ se budou shodovat s prvky Ω, kde λ je libovolné celé číslo, které není dělitelné číslem n.“ (Gauss 1986, s. 415) Smyslem Gaussova řešení je rozdělit kořeny do period, tedy součtů kořenů, ve kterých každý následující prvek je g-tá mocnina předešlého prvku a g-tá mocnina posledního prvku v součtu je znovu výsledkem prvního prvku[17]. „Jestliže e je dělitelem čísla $n-1$, položíme $n - 1 = fe$, kde f je počet kořenů v periodě, g^e označíme h. […] Součet f takových kořenů je

$$[\lambda] + [\lambda h] + \cdots + [\lambda h^{f-1}] = (f, \lambda)$$

Množina kořenů v (f, λ) se nazývá ***perioda*** (f, λ).“ (Gauss 1986, s. 415) Dále Gauss vymezuje vlastnosti definovaných period: „Jestliže $f = n - 1$, $e = 1$, perioda $(f, 1)$

[16] Pro větší přehlednost jsme změnili značení, místo původního *r* píšeme ε a místo *x* píšeme *t*.
[17] V dnešní době je to označení pro cyklickou grupu.

se bude shodovat s Ω. Ve zbývajících případech se bude Ω skládat z period $(f,1)$, (f,g), $(f,g^2),\ldots,(f,g^{e-1})$. Proto tyto periody budou navzájem různé a každá podobná perioda (f,λ) se bude shodovat s jednou z těchto period, jestliže $[\lambda]$ patří do Ω a λ není dělitelná číslem n." (Gauss 1968, s. 416)

„Pokud je $n-1=a\cdot b\cdot c$, pak perioda (bc,λ) se skládá z b period (c,λ):

$$(bc,\lambda)=(c,\lambda)+(c,\lambda g^{a})+(c,\lambda g^{2a})+\cdots\left(c,\lambda g^{a(b-1)}\right) \qquad (3)$$

Jestliže se tedy číslo $n-1$ dá rozložit na součin prvočísel α,β,γ, atd., jejich počet označíme v, pak určení kořenů rovnice (1) zredukujeme na řešení v rovnic stupně α,β,γ, atd." (Gauss 1986, s. 416)

První perioda obsahuje $\frac{n-1}{\alpha}=r$ prvků. Druhá perioda obsahuje pouze $\frac{n-1}{\alpha\beta}=s$, přičemž $h=g^{re}$. Další perioda pak $\frac{n-1}{\alpha\beta\gamma}$ prvků a $h=g^{rse}$, atd.

Vezměme $n=17$, rovnice (1) pak bude mít tvar $t^{16}+t^{15}+\cdots+t+1$.

Dále $n-1=16=2\cdot2\cdot2\cdot2$, dostaneme tedy 4 kvadratické rovnice. Číslo 3 je podle Gausse primitivním kořenem 17, tedy mocniny čísla 3 *mod* 17 jsou všechna čísla 1, 2, …, 16.[18] Nejmenší zbytky mocnin čísla 3 vzhledem k modulo 17 jsou shrnuty v následující tabulce, v prvním řádku jsou exponenty mocnin, v druhém pak nejmenší zbytky (Gauss 1986, s. 432).

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Hodnoty v druhém řádku tabulky jsme získali takto: $3^0=1$; $3^1=3$; $3^2=9$; $3\cdot9=27\equiv10\ mod\ 17$; $3\cdot10=30\equiv13\ mod\ 17$; $3\cdot13=39\equiv5\ mod\ 17$; $3\cdot5=15$; $3\cdot15=45\equiv11\ mod\ 17$; $3\cdot11=33\equiv16\ mod\ 17$; atd.

Periodu $(16,1)$ zapíšeme jako součet mocnin čísla 3 *mod* 17:

$$(16,1)=[1]+[3]+[9]+[10]+[13]+[5]+[15]+[11]+[16]+[14]+[8]+[7]+[4]+[12]+[2]+[6]$$

[18] Vytvoříme cyklickou grupu modulo 17.

Dále pak podle vztahu (3) můžeme zapsat periodu $(16,1)$ jako 2 periody $(8,\lambda)$, protože $n-1 = a \cdot b \cdot c = 1 \cdot 2 \cdot 8$

$$(16,1) = 2(8,1) = (8,1) + \big(8,(1 \cdot 3^1)\big) = (8,1) + (8,3)$$

Protože z definice pro periodu zjistíme e: $16 = f \cdot e = 8 \cdot 2$, je $h = g^e = 3^2 = 9$. Periody $(8,1)$ a $(8,3)$ můžeme pak zapsat jako součty kořenů:

$$\begin{aligned}(8,1) &= [1] + [9] + [9^2] + [9^3] + [9^4] + [9^5] + [9^6] + [9^7] \\ &= [1] + [9] + [13] + [15] + [16] + [8] + [4] + [2] \\ (8,3) &= [3] + [3 \cdot 9] + [3 \cdot 9^2] + [3 \cdot 9^3] + [3 \cdot 9^4] + [3 \cdot 9^5] + [3 \cdot 9^6] + [3 \cdot 9^7] \\ &= [3] + [10] + [5] + [11] + [14] + [7] + [12] + [6]\end{aligned}$$

Periody $(8,1)$ a $(8,3)$ můžeme dále rozepsat na součet, $h = 3^2$.

$$(8,1) = 2(4,1) = (4,1) + \big(4,(1 \cdot 9)\big) = (4,1) + (4,9)$$

$$(8,3) = 2(4,3) = (4,3) + \big(4,(3 \cdot 9)\big) = (4,3) + (4,10)$$

Pro periody $(4,1),(4,9),(4,3),(4,10)$ je $g = 3^4 \equiv 13\ mod\ 17$.

$$\begin{aligned}(4,1) &= [1] + [13] + [13^2] + [13^3] = [1] + [13] + [16] + [4] \\ (4,9) &= [9] + [9 \cdot 13] + [9 \cdot 13^2] + [9 \cdot 13^3] = [9] + [15] + [8] + [2] \\ (4,3) &= [3] + [3 \cdot 13] + [3 \cdot 13^2] + [3 \cdot 13^3] = [3] + [5] + [14] + [12] \\ (4,10) &= [10] + [10 \cdot 13] + [10 \cdot 13^2] + [10 \cdot 13^3] = [10] + [11] + [7] + [6]\end{aligned}$$

$$(4,1) = (2,1) + (2,13)$$

$$(4,9) = (2,9) + (2,15)$$

$$(4,3) = (2,3) + (2,5)$$

$$(4,10) = (2,10) + (2,11)$$

Nyní už dostáváme samotné kořeny, $g = 3^8 = 16$:

$$(2,1) = [1] + [16]$$

$$(2,13) = [4] + [13]$$

$$(2,9) = [8] + [9]$$

$$(2,15) = [2] + [15]$$

$$(2,3) = [3] + [14]$$

$$(2,5) = [5] + [12]$$

$$(2,10) = [7] + [10]$$

$$(2,11) = [6] + [11]$$

Dále potřebujeme sestavit samotné kvadratické rovnice, periody $(8,1) = x_1$, $(8,3) = x_2$ přepíšeme do tvaru s kořeny $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{16}$. Budeme při tom vycházet ze zjednodušené verze Gaussova výpočtu v knize *Galois Theory* (Stewart 2004, str. 220–222).

$$x_1 = \varepsilon + \varepsilon_9 + \varepsilon_{13} + \varepsilon_{15} + \varepsilon_{16} + \varepsilon_8 + \varepsilon_4 + \varepsilon_2$$
$$x_2 = \varepsilon_3 + \varepsilon_{10} + \varepsilon_5 + \varepsilon_{11} + \varepsilon_{14} + \varepsilon_7 + \varepsilon_{12} + \varepsilon_6$$

Protože vrcholy ε_k, ε_{17-k} jsou symetrické vzhledem k reálné ose, platí

$$\varepsilon_k + \varepsilon_{17-k} = 2\cos k\theta, \quad k = 1, \dots, 16 \tag{5}$$

Ze vztahu (5) pak vyplývají rovnosti:

$$x_1 = 2(\cos\theta + \cos 2\theta + \cos 4\theta + \cos 8\theta)$$
$$x_2 = 2(\cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta)$$

Odtud, pokud ještě využijeme vztah $2\cos a\theta \cos b\theta = \cos(a+b)\theta + \cos(a-b)\theta$, dostáváme $x_1 \cdot x_2 = -4$. Když sečteme všechny kořeny, dostaneme hodnotu -1, tedy $x_1 + x_2 = -1$. Z těchto vztahů[19] dostaneme následující kvadratickou rovnici:

$$t^2 + t - 4 = 0 \tag{6}$$

Dále $x_1 > 0$, takže $x_1 > x_2$, kořeny kvadratické rovnice (6) tedy jsou

$$x_1 = \frac{-1 + \sqrt{17}}{2}$$
$$x_2 = \frac{-1 - \sqrt{17}}{2}$$

Čtyř prvkové periody můžeme zapsat tímto způsobem:

$$u_1 = \varepsilon + \varepsilon_{13} + \varepsilon_{16} + \varepsilon_4 = 2(\cos\theta + \cos 4\theta)$$
$$u_2 = \varepsilon_9 + \varepsilon_{15} + \varepsilon_8 + \varepsilon_2 = 2(\cos 2\theta + \cos 8\theta)$$
$$v_1 = \varepsilon_3 + \varepsilon_5 + \varepsilon_{14} + \varepsilon_{12} = 2(\cos 3\theta + \cos 5\theta)$$
$$v_2 = \varepsilon_{10} + \varepsilon_{11} + \varepsilon_7 + \varepsilon_6 = 2(\cos 6\theta + \cos 7\theta)$$

Z těchto rovností odvodíme že, $u_1 > u_2$ a $v_1 > v_2$.

Abychom mohli opět sestavit kvadratické rovnice, potřebujeme $u_1 + u_2 = x_1$, $v_1 + v_2 = x_2$. Dále platí

$$u_1 \cdot u_2 = \varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{16} = -1$$

[19] Využijeme Vietovy vztahy pro kvadratickou rovnici.

$$v_1 \cdot v_2 = \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_{16} = -1$$

Hledané kvadratické rovnice pak jsou:

$$t^2 - x_1 t - 1 = 0 \tag{7}$$

$$t^2 - x_2 t - 1 = 0 \tag{8}$$

Z kvadratických rovnic dostáváme kořeny:

$$u_1 = \frac{x_1 + \sqrt{x_1^2 + 4}}{2} = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{4}$$

$$u_2 = \frac{x_1 - \sqrt{x_1^2 + 4}}{2} = \frac{-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}}{4}$$

$$v_1 = \frac{x_2 + \sqrt{x_2^2 + 4}}{2} = \frac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{4}$$

$$v_2 = \frac{x_2 - \sqrt{x_2^2 + 4}}{2} = \frac{-1 - \sqrt{17} - \sqrt{34 + 2\sqrt{17}}}{4}$$

Z dvojčlenných period nám stačí pouze dvě:

$$w_1 = \varepsilon_1 + \varepsilon_{16}$$

$$w_2 = \varepsilon_{13} + \varepsilon_4$$

Pro sestavení příslušné kvadratické rovnice je třeba vědět, že $w_1 + w_2 = u_1$

a $w_1 w_2 = \varepsilon_3 + \varepsilon_5 + \varepsilon_{14} + \varepsilon_{12} = v_1$.

Dále víme, že $w_1 > w_2$, protože podle (5) máme:

$$w_1 = 2\cos\theta$$

$$w_2 = 2\cos 4\theta$$

Můžeme sestavit kvadratickou rovnici[20]:

$$t^2 - u_1 t + v_1 = 0 \tag{9}$$

Vyjádříme si pouze w_1 (w_2 se vypočítá analogicky).

$$w_1 = \frac{u_1 + \sqrt{u_1^2 - 4v_1}}{2}$$

Protože $\cos\theta = \frac{w_1}{2}$, dostáváme velikost $\cos\theta$:

[20] Z dvojčlenných period bychom dostali celkem 4 kvadratické rovnice.

$$\cos\frac{2\pi}{17} = \frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\right.$$
$$\left. + \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2\left(1 - \sqrt{17}\right)\sqrt{34 - 2\sqrt{17}}}\right)$$

Jak je vidět, $\cos\frac{2\pi}{17}$ opravdu lze sestrojit, neboť číselný výraz na pravé straně se skládá pouze z algebraických operací a z druhé odmocniny.

3.1.2 Serretova konstrukce

Nyní si předvedeme konstrukci založenou přímo na Gaussových periodách, která pro sestrojení pravidelného 17-úhelníku využívá kružnic. Budeme vycházet z článku *O pravidelném 17-úhelníku* (Strnad 1904). Poprvé tuto konstrukci ale zveřejnil francouzský matematik *Joseph Alfred Serret* (1819-1885) v díle *Cours d'algèbre supérieure* (2. ed. 1854), upravil ji pak *Paul Gustav Heinrich Bachmann* (1837–1920) ve své knize *Die Lehre von der Kreistheilung* (1872).

V pravoúhlé soustavě souřadnic s osami x, y sestrojíme kružnici k o poloměru 1 se středem v bodě $O = (0,\ 0)$. Tato kružnice protne osu y v bodě $(0,\ 1)$, což je vrchol A_0 (obr. 4).

Průměr jednotkové kružnice označíme $|A_0B| = 2$. Hodnota w_1, kterou jsme získali výpočtem z kvadratické rovnice (9) je délka tětivy BA_2 kružnice k. Strana a pravidelného 17-úhelníku vepsaného do kružnice k pak vypadá následovně:

$$a = 2\sin\frac{\theta}{2} = 2\sqrt{\frac{1 - \cos\theta}{2}} = \sqrt{2 - w_1}$$

Nejdříve sestrojíme $|OF| = -\frac{1}{4}$, znaménkem mínus pouze vyjadřujeme, že velikost $\frac{1}{4}$ vyznačíme v záporném směru osy x.

Z Pythagorovy věty pro trojúhelník A_0OF získáme

$$|A_0F| = \sqrt{|A_0O|^2 + |FO|^2} = \frac{1}{4}\sqrt{17}$$

Kružnice $k_1 = (F, |A_0F|)$ protne osu x v bodech G, H tak, že platí

$$|OG| = |FG| - \frac{1}{4} = \frac{\sqrt{17}-1}{4} = \frac{x_1}{2}$$

$$|OH| = -|FG| - \frac{1}{4} = \frac{-\sqrt{17}-1}{4} = \frac{x_2}{2}$$

x_1, x_2 jsou kořeny rovnice (6).

Využitím Pythagorovy věty pro trojúhelník A_0OG zjistíme velikost

$$|A_0G| = \sqrt{|A_0O|^2 + |OG|^2} = \sqrt{\frac{x_1^2}{4} + 1}$$

Dále sestojíme kružnici $k_2 = (G, |A_0G|)$, která určí body J, K jako její průsečíky s osou x.

$$|OJ| = |OG| + |GJ| = \frac{x_1}{2} + \sqrt{\frac{x_1^2}{4} + 1} = u_1$$

$$|OK| = |OG| - |GK| = \frac{x_1}{2} - \sqrt{\frac{x_1^2}{4} + 1} = u_2$$

u_1, u_2 jsou kořeny rovnice (7).

Díky kružnici $k_3 = (H, |A_0H|)$ dostaneme na ose x body $L,\ M$.

$$|OL| = \frac{x_2}{2} + \sqrt{\frac{x_2^2}{4} + 1} = v_1$$

$$|OM| = \frac{x_2}{2} - \sqrt{\frac{x_2^2}{4} + 1} = v_2$$

v_1, v_2 jsou kořeny kvadratické rovnice (8).

Nyní chceme sestrojit hodnoty w_1, w_2. Označíme si bod $D = (-1, 0)$. Nad průměrem $|DL|$ opíšeme polokružnici k_4, která protne osu y v bodě N. Podle Euklidovy věty o výšce pro trojúhelník DLN platí: $|ON|^2 = |DO|\,.\,|OL|$, tedy $|ON| = \sqrt{v_1}$. Dále sestrojíme kružnici $k_5 = \left(N, \frac{1}{2}|OJ|\right)$, její průsečík s osou x označíme P, přičemž platí:

$$|NP| = \frac{1}{2}|OJ| = \frac{u_1}{2}$$

Zároveň v trojúhelníku OPN je velikost strany OP podle Pythagorovy věty:

$$|OP| = \sqrt{|NP|^2 - |ON|^2} = \sqrt{\frac{u_1^2}{4} - v_1}$$

Kružnice $k_6 = (P, |NP|)$ protíná osu x v bodech $Q,\ R$ tak, že platí:

$$|OQ| = |OP| + |PQ| = \frac{u_1}{2} + \sqrt{\frac{u_1^2}{4} - v_1} = w_1$$

$$|OR| = |OP| - |PR| = \frac{u_1}{2} - \sqrt{\frac{u_1^2}{4} - v_1} = w_2$$

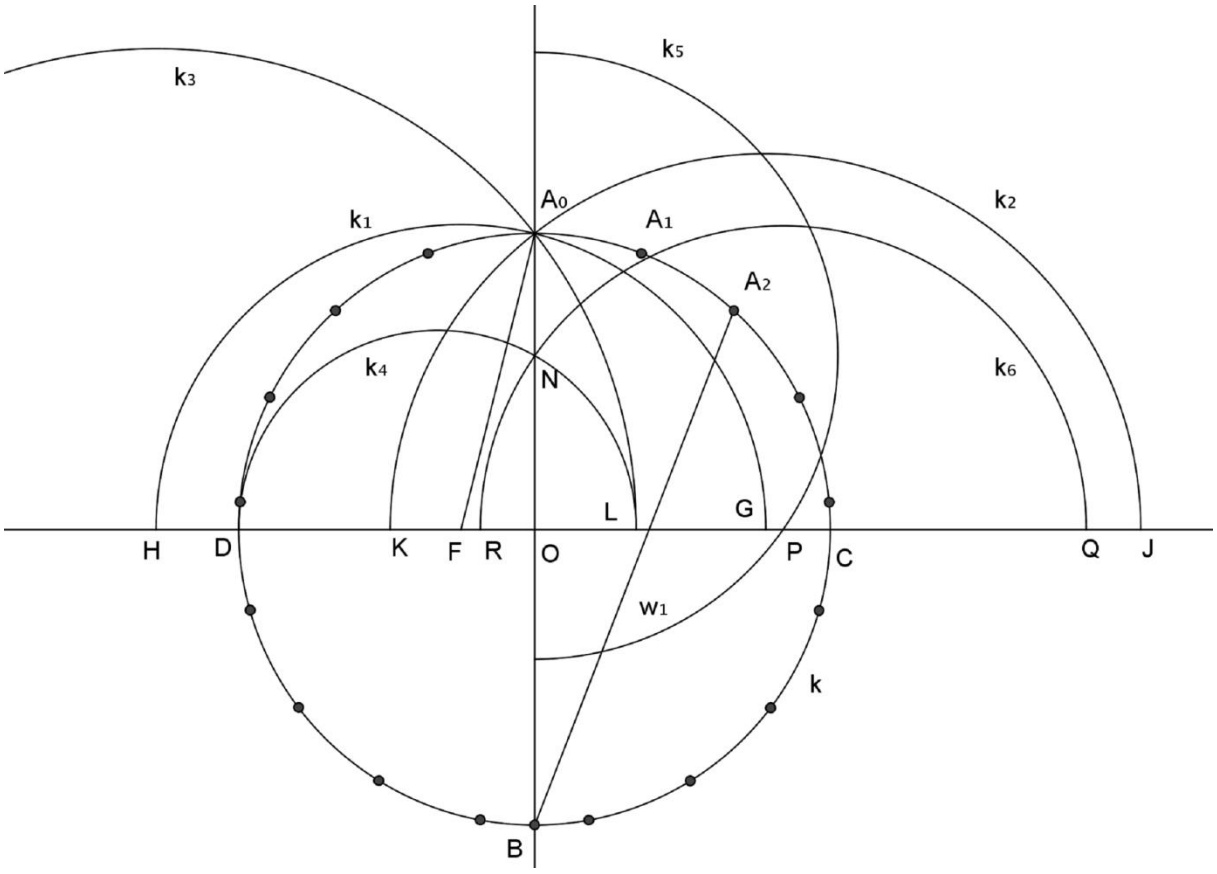
w_1, w_2 jsou kořeny rovnice (9).

Tím jsme prakticky hotovi. V kružnici k sestrojíme tětivu $|BA_2| = w_1$. Rozpůlíme oblouk A_0A_2, tím dostaneme bod A_1, neboť jak víme

$$w_1 = 2\cos\theta$$

$$|\sphericalangle A_0BA_2| = |\sphericalangle A_0OA_1| = \theta = \frac{2\pi}{17}$$

Nyní jsme již schopni sestrojit všechny vrcholy $A_0, A_1, \ldots, A_{16}$ pravidelného 17-úhelníku.



Obr. 4.: Konstrukce pravidelného 17-úhelníku (Serret)

3.1.3 Lowryho konstrukce

Po vydání Gaussova důkazu sestrojitelnosti pravidelného 17-úhelníku se mnoho matematiků zajímalo o samotnou konstrukci tohoto mnohoúhelníku, do dnešní doby jich existuje celá řada. Někteří modifikovali původní konstrukce, jiní vymýšleli stále nové způsoby tak, aby daná konstrukce byla co nejjednodušší. Jedním z prvních, komu se to podařilo, byl *Samuel James*, který podal čistě geometrickou konstrukci a důkaz v roce 1819 v *Transactions of the Irish Academy*. V roce 1825 napsal Gauss oznámení[21], že *Johannes Erchinger* (1788–1829) podal čistě geometrickou konstrukci pravidelného 17-úhelníku. Tato konstrukce je popsána v článku *Remarks on Klein's "Famous Problems of Elementary Geometry* (Archibald 1914, s. 252).

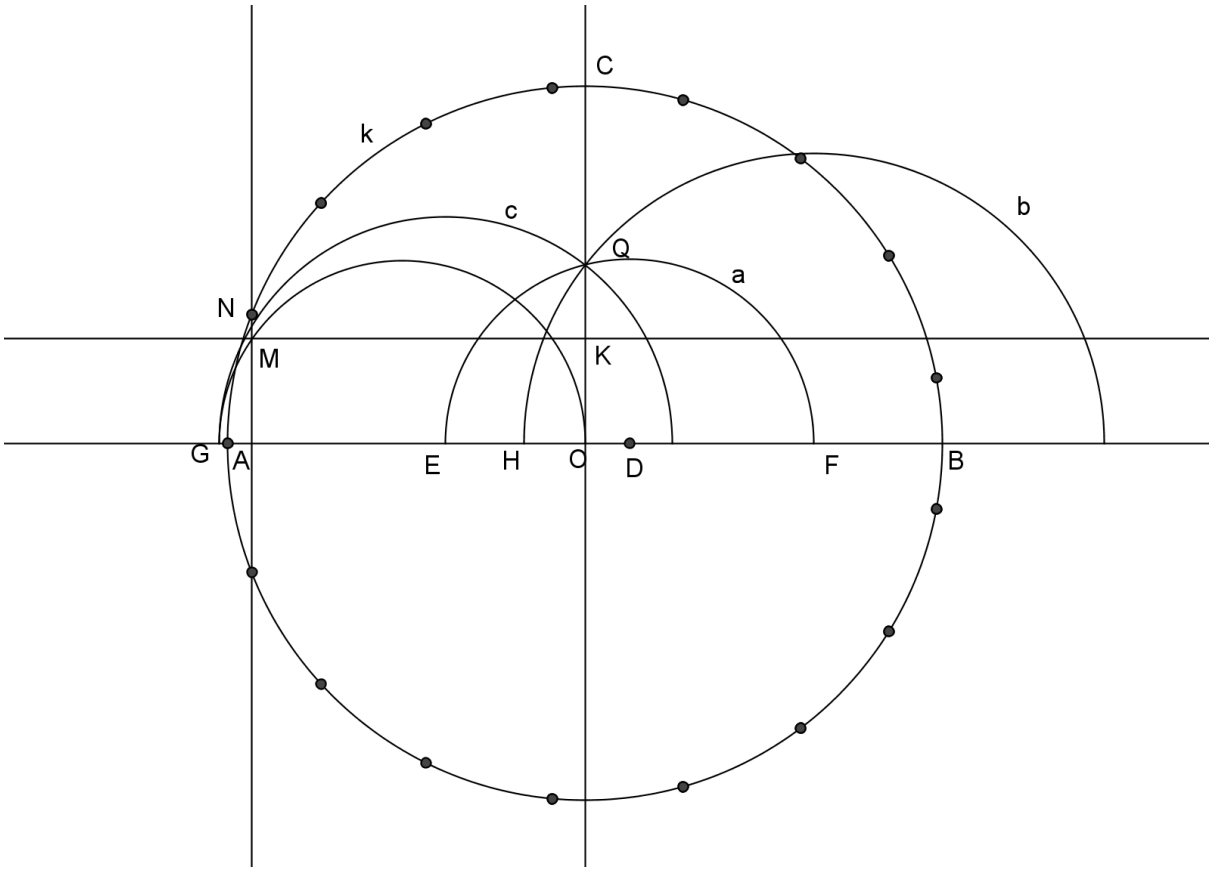
Zde si přiblížíme konstrukci, kterou popsal *John Lowry* v roce 1819 v nové řadě časopisu *The Mathematical Repository*. Při její interpretaci budeme vycházet z článku (Archibald 1914, s. 252).

[21] *Göttingische gelehrte Anzeigen*, 19. prosince 1825 (Archibald 1914, s. 252).

Nejdříve sestrojíme kružnici k nad libovolným průměrem AB, střed úsečky AB označíme O, bodem O vedeme kolmici na úsečku AB, ta nám protne kružnici k v bodě C (obr. 5). Na OB sestrojíme bod D tak, že $|OD| = \frac{1}{8}|OB|$, na OC sestrojíme bod Q tak, aby platilo $|OQ| = \frac{1}{2}|OC|$. Dále sestrojíme body E, F takové, že $|DQ| = |DE| = |DF|$, využijeme proto kružnici $a = (D, |DQ|)$, její průsečíky s AB nám dají hledané body E, F. Průsečík kružnice $b = (F, |FQ|)$ a přímky AB, který leží uvnitř úsečky AB, nazveme H, průsečík kružnice $c = (E, |EQ|)$ s přímkou AB, který leží vně úsečky AB, nazveme G. Na úsečce OC sestrojíme bod K tak, aby splňoval vztah

$$|OK| = \sqrt{|OH| \,.\, |OQ|}$$

Bodem K vedeme rovnoběžku s AB, ta se nám protne s polokružnicí sestrojenou nad průměrem OG v bodě M. Bodem M potom vedeme rovnoběžku s OC, která se protne s kružnicí k v bodě N. $|AN|$ je velikostí strany pravidelného 17-úhelníku vepsaného do kružnice k sestrojené nad průměrem AB.



Obr. 5: Konstrukce pravidelného 17-úhelníku (Lowry)

3.1.4 Rychlíkova konstrukce

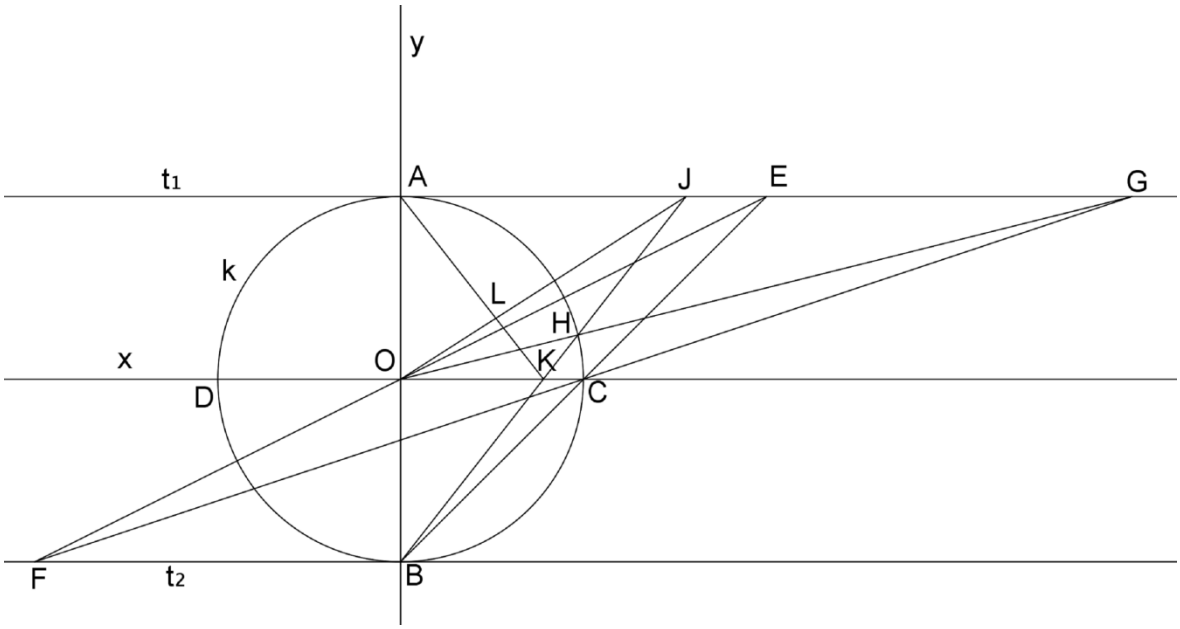
Jak popisuje *Strnad* ve svém článku *O pravidelném sedmnáctiúhelníku* (Strnad 1904, s. 551), konstrukci založenou na goniometrických úvahách vydal v roce 1812 *Adrien-Marie Legendre* v *Eléments de géométrie*. *André-Marie Ampère* pak využil ke své konstrukci planimetrické relace, popsal ji v roce 1835 v *Comptes rendus*. Dalším, kdo se zabýval konstrukcí pravidelného 17-úhelníku byl *Christian von Staudt*, kterému se podařilo sestrojit daný mnohoúhelník pomocí jedné kružnice a soustavy přímek, svůj objev vydal roku 1842 v *Crelle's Journal*. V tom samém časopise, ale o 30 let později, tedy v roce 1872 publikoval *Heinrich Schröder*, zjednodušené řešení Staudtovy konstrukce. *Louis Gérard* popsal roku 1897 v *Mathematische Annalen*, sestrojení pravidelného 17-úhelníku pouze pomocí kružnic na způsob *Mascheroniho* konstrukce. Naším cílem však není vyjmenovat všechny autory, kteří se zasloužili o objevení nových konstrukcí pravidelného 17-úhelníku, neboť jich je opravdu mnoho.

Nyní opíšeme konstrukci pomocí jedné pevně zadané kružnice se středem a pomocí přímek, kterou popsal *Karel Rychlík* a je založená na *Schröderově* konstrukci (Rychlík 1912). Grafické znázornění konstrukce rozdělíme kvůli lepší přehlednosti na dvě části, v popisu pak vyznačíme, kde začíná druhý obrázek.

Nejdříve sestrojíme předem danou kružnici k se středem O a poloměrem r, poté narýsujeme dva navzájem kolmé průměry, označíme je CD a AB (obr. 6). V bodech A, B narýsujeme tečny t_1, t_2 ke kružnici k. Nejprve chceme najít bod G, pro který platí $|AG| = 4$ (předpokládáme, že poloměr $r = 1$). Za tímto účelem povedeme přímku BC, která protne tečnu t_1 v bodě E, poté sestrojíme polopřímku EO, její průsečík s tečnou t_2 nazveme F. Polopřímka FC protne tečnu t_1 v hledaném bodě G.

Nyní chceme sestrojit $|\sphericalangle AON| = 2\delta$ (pro úhel δ platí $tg4\delta = 4$)[22]. Polopřímka OG protne kružnici k v bodě H. Pro úhel ABH platí, že $|\sphericalangle ABH| = 2\delta$. Polopřímka BH protne tečnu t_1 v bodě J a přímku x v bodě K. Průsečík úsečky OJ a úsečky KA označíme L.

[22] Viz následující *Richmondovu* konstrukci.

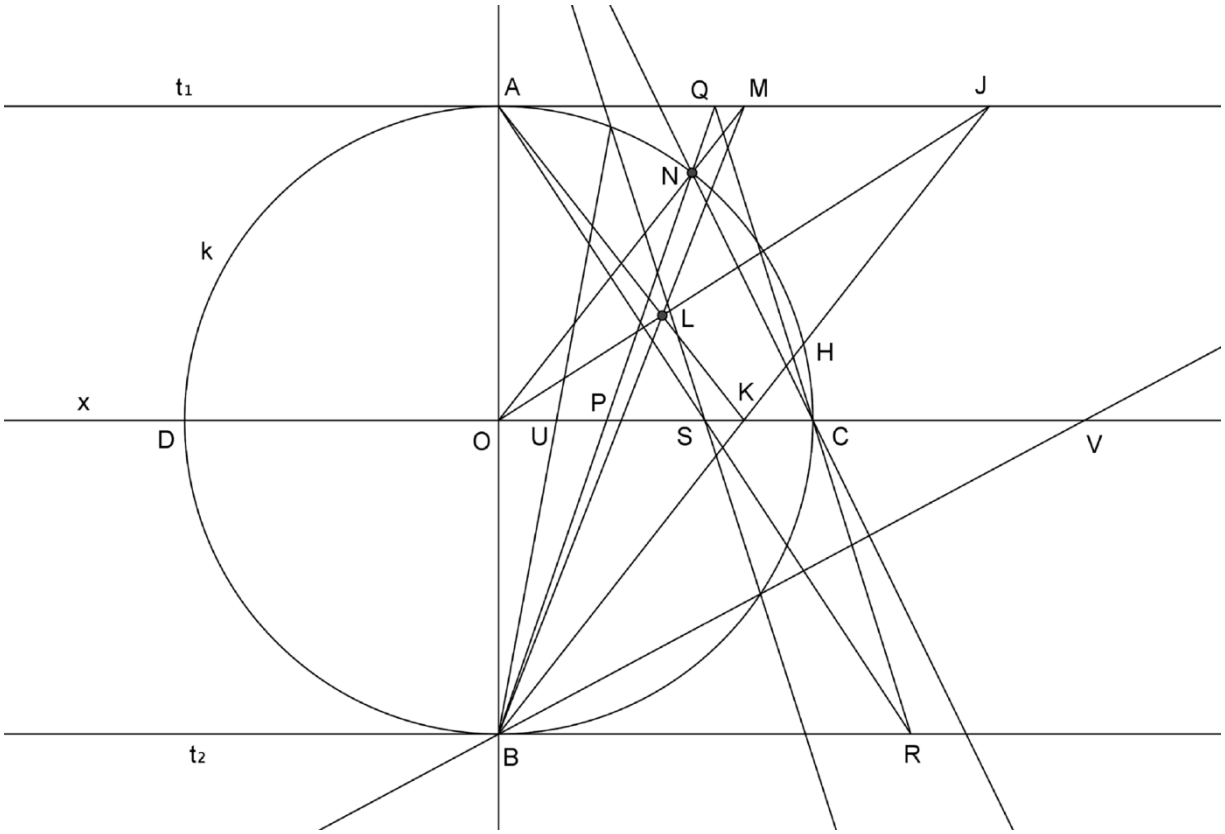


Obr. 6: Konstrukce pravidelného sedmnáctiúhelníku pomocí pevné kružnice

Dále spojíme bod L s bodem B (obr. 7), přímka LB protne tečnu t_1 v bodě M. Polopřímka OM protne kružnici k v bodě N. Přímka ON je rovnoběžná s přímkou BH a tedy $|\sphericalangle AON| = 2\delta$. Průsečík úsečky BN s přímkou x je bod P a průsečík polopřímky CN s přímkou y označíme bodem T. Nyní potřebujeme přenést úsečku OP do polohy SC, což uděláme následovně: Polopřímka BN protne tečnu t_1 v bodě Q a polopřímka QC protne tečnu t_2 v bodě R. Průsečík přímky AR s přímkou x bude bod S. Nyní bod S spojíme s bodem T. Průsečíky kružnice k s přímkou ST spojíme s bodem B, na přímce x tak získáme body U, V.

$$|OU| = 2\cos 4\theta$$
$$|OV| = 2\cos\theta = w_1$$

Velikost w_1 jsme již použili v *Serretově* konstrukci, str. 41–43. Tím jsme vlastně hotovi, jednotlivé vrcholy pravidelného 17-úhelníku jsme už schopni najít.



Obr. 7: Konstrukce pravidelného 17-úhelníku pomocí pevné kružnice (dokončení)

3.1.5 Richmondova konstrukce

Mezi nejjednodušší konstrukce popsané do dnešní doby patří konstrukce Richmondova, kterou si nyní popíšeme blíže. Vycházíme z knihy *Galois Theory* (Stewart 2004, s. 222–223). *Herbert William Richmond* (1863–1948) založil svoji konstrukci pravidelného sedmnáctiúhelníku na dělení úhlu na čtyři stejné díly. Zároveň vychází z Gaussova algebraického výpočtu, který jsme popsali dříve. Nechť tedy δ je nejmenší kladný ostrý úhel takový, že $tg\ 4\delta = 4$, pak i $\delta,\ 2\delta,\ 4\delta$ jsou ostré úhly. Rovnici[23]

$$t^2 + t - 4 = 0$$

můžeme napsat ve tvaru

$$t^2 + 4t\ cotg\ 4\delta - 4 = 0$$

Kořeny této rovnice jsou

$$x_1 = 2tg\ 2\delta$$
$$x_2 = -2cotg\ 2\delta$$

[23] Rovnice (6) z algebraického výpočtu strany pravidelného 17-úhelníku, str. 42.

Pak ale $u_1,\ u_2,\ v_1,\ v_2$ můžeme vyjádřit ve tvaru

$$u_1 = tg\left(\delta + \frac{\pi}{4}\right)$$

$$u_2 = tg\left(\delta - \frac{\pi}{4}\right)$$

$$v_1 = tg\ \delta$$

$$v_2 = -cotg\ \delta$$

Potom z původního algebraického výpočtu a ze vztahu

$$2\cos a\theta \cos b\theta = \cos(a+b)\theta + \cos(a-b)\theta$$

vyplývá, že

$$2(\cos 3\theta + \cos 5\theta) = tg\ \delta$$

$$4\cos 3\theta\ \cos 5\theta = tg\left(\delta - \frac{\pi}{4}\right)$$

Nyní přistoupíme ke grafickému znázornění konstrukce (obr. 8). Nechť OC a OA jsou dva navzájem kolmé poloměry kružnice k. Najdeme bod J tak, že $|OJ| = \frac{1}{4}|OA|$, a bod E, pro který platí $|\sphericalangle OJE| = \frac{1}{4}|\sphericalangle OJC|$. Dále sestrojíme bod F na úsečce OC takový, aby $|\sphericalangle OJF| = \frac{\pi}{4}$. Polokružnice nad průměrem FC protne OA v bodě K. Kružnice $m = (E, |EK|)$ protne průměr DC v bodech N_3, N_5, v těchto bodech pak vedeme kolmice na OC, jejich průsečíky s kružnicí k nazveme A_3, A_5. Pro úhel OJC platí $|\sphericalangle OJC| = 4\delta$, tudíž $|\sphericalangle OJE| = \delta$. Zároveň platí následující vztahy

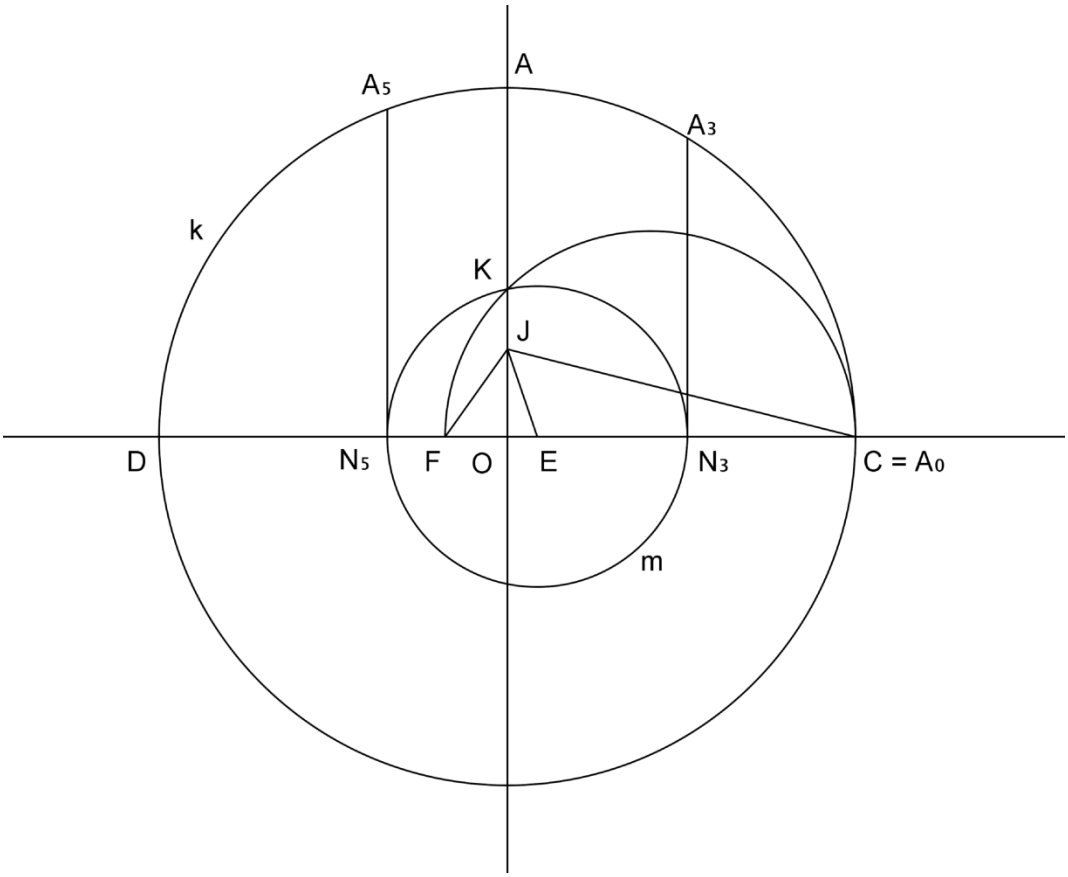
$$2(\cos|\sphericalangle COA_3| + \cos|\sphericalangle COA_5|) = 2\frac{|ON_3| - |ON_5|}{|OC|} = 4\frac{|OE|}{|OC|} + \frac{|OE|}{|OJ|} = tg\ \delta$$

$$4\cos|\sphericalangle COA_3|\cos|\sphericalangle COA_5| = -4\frac{|ON_3|\,.\,|ON_5|}{|OC|\,.\,|OC|}$$

$$= -4\frac{|OK|^2}{|OC|^2} = -4\frac{|OF|}{|OC|} = -\frac{|OF|}{|OJ|} = tg\left(\delta - \frac{\pi}{4}\right)$$

Tedy $|\sphericalangle COA_3| = 3\theta$ a $|\sphericalangle COA_5| = 5\theta$.

Tím jsme získali vrcholy $C = A_0$, A_3, A_5 pravidelného 17-úhelníku, který již z těchto vrcholů dokážeme sestrojit. Z nalezených vrcholů si vybereme jednu dvojici a postupně nanášíme jejich vzdálenost na kružnici k. Tímto způsobem jsme schopni nalézt všechny vrcholy.



Obr 8: Konstrukce pravidelného 17-úhelníku (Richmond)

Závěr

Cílem práce bylo dokázat větu vymezující konstruovatelné pravidelné mnohoúhelníky, vysvětlit Gaussovu konstrukci pravidelného 17-úhelníku a popsat některé další konstrukce od jiných autorů.

Věta, která charakterizuje, kdy je pravidelný *n*-úhelník konstruovatelný a kdy nikoli, je známá jako Gaussova věta. V bakalářské práci jsme ji dokázali přes Galoisovu teorii, nejdříve bylo tedy třeba, abychom vysvětlili zásadní pojmy této teorie, které jsme při důkazu využili, také jsme vyslovili a algebraicky dokázali důležité věty o konstruovatelnosti kružítkem a pravítkem.

V další kapitole jsme vysvětlili Gaussův teoretický výpočet strany pravidelného 17-úhelníku. Zároveň jsme podali hned několik konstrukcí tohoto mnohoúhelníku od různých autorů, zabývali jsme se i podrobným objasněním jednotlivých sestrojení, která jsme doplnili i názornými obrázky. Každá konstrukce je založena na jiném principu, na druhé straně jsou ale téměř všechny vzájemně propojeny, vycházejí ze stejných algebraických vyjádření.

Zadané cíle se nám tedy podařilo splnit.

Některé konstrukce jsou natolik srozumitelné, že je můžeme využít i na střední škole, v čemž vidíme velký přínos této práce.

Dalším přínosem je určitě spojení algebry a geometrie do jednoho celku. Matematika je sice věda, která se dělí na zdánlivě odlišné obory, které většinou fungují nezávisle na sobě. Ve skutečnosti ale jsou tato odvětví propojená, vzájemně si pomáhají a ovlivňují se. Tato práce je příkladem toho, jak teorie z jednoho matematického oboru dokáže vyřešit úlohu zadanou v oboru jiném, neboť typicky geometrickou úlohu o sestrojení pravidelného mnohoúhelníku řešíme pomocí čistě algebraických prostředků. Zároveň zde podáváme i ryze geometrickou konstrukci. Spojujeme zde tedy pod jedním tématem algebru a geometrii dohromady.

Seznam použité literatury

ARCHIBALD, Raymond Clare. Gauss and the regular polygon of seventeen sides. *The American Mathematical Monthly*. 1920, roč. 27, č. 7/9, s. 323-326. ISSN: 0002-9890. Dostupné z: http://poncelet.math.nthu.edu.tw/disk5/js/geometry/archibald.pdf

ARCHIBALD, Raymond Clare. Remarks on Klein's "Famous Problems of Elementary Geometry. *The American Mathematical Monthly*. 1914, roč. 21, č. 8, s. 247-259. ISSN: 0002-9890. Dostupné z: http://poncelet.math.nthu.edu.tw/disk5/js/geometry/remarks.pdf

BIERMANN, Kurt R. Thomas Clausen, Mathematiker und Astronom. J*ournal für die reine und angewandte Mathematik*. 1964, č. 216, s. 159-198. ISSN 0075-4102.

BŰHLER, Walter Kaufmann. *Gauss: A Biographical Study*. 2. vyd. New York: Springer-Verlag, 1987. ISBN 3-540-10662-6.

COURANT, Richard a Herbert ROBBINS. *What is Mathematics?: An Elementary Approach to Ideas and Methods*. 2. vyd. New York, Oxford: Oxford University Press, 1996. ISBN 978-0-19-510519-3.

DUNNINGTON, Waldo. The Sesquicentennial of the Birth of Gauss. *The Scientific Monthly*. 1927, roč. 24, č. 5, s. 402-414. DOI: 10.2307/7912. Dostupné z: http://www.jstor.org/stable/7912

EUKLEIDES. *Základy Knihy I-IV*. Editor: Petr Vopěnka. Nymburk: OPS, 2007. ISBN 978-80-903773-7-0.

GAUSS, Carl Friedrich. *Disquisitiones Arithmeticae*. Překlad: Arthur A. CLARKE. 2. přetištěné vyd. New York Berlin Heidelberg Tokyo: Springer-Verlag, 1986. ISBN 0-387-96254-9.

KLEIN, Felix. *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert: Teile 1 und 2*. Přetištěné vydání. Berlin Heidelberg New York: Springer-Verlag, 1979. ISBN 3-540-09234-X. Dostupné z: http://gdz.sub.uni-goettingen.de/dms/load/img/?PPN=PPN375425993&DMDID=DMDLOG_0001&LOGID=LOG_0001&PHYSID=PHYS_0003

KOŘISTKA, Karel František Edvard. O pracích a vynálezech Gaussových v oboru geodaesie. *Časopis pro pěstování matematiky a fysiky*. 1877, roč. 6, č. 4, s. 174–183. ISSN: 1802-114X. Dostupné z: http://dml.cz/dmlcz/123682

KOŘÍNEK, Vladimír. *Základy algebry*. 2. vyd. Praha: Nakladatelství Československé akademie věd, 1956.

KŘÍŽEK, Michal. Od Fermatových čísel ke geometrii. *Pokroky matematiky, fyziky a astronomie*. 2001, roč. 46, č. 3, s. 179-191. ISSN 0032-2423. Dostupné z: http://dml.cz/dmlcz/141082

KŘÍŽEK, Michal. O Fermatových číslech. *Pokroky matematiky, fyziky a astronomie*. 1995, roč. 40, č. 5, s. 243-253. ISSN 0032-2423. Dostupné z: http://dml.cz/dmlcz/138304

POLÁK, Josef. *Přehled středoškolské matematiky*. 9. přepracované vyd. Praha: Prometheus, 2008. ISBN 978-80-7196-356-1.

RYCHLÍK, Karel. Sestrojení pravidelného sedmnáctiúhelníku. *Časopis pro pěstování matematiky a fysiky*. 1912, roč. 41, č. 1, s. 81-93. ISSN: 1802-114X. Dostupné z: http://dml.cz/dmlcz/122211

SEYDLER, August. O Gaussových pracích fysikálních. *Časopis pro pěstování matematiky a fysiky*. 1877, roč. 6, č. 4, s. 191-196. ISSN: 1802-114X. Dostupné z: http://dml.cz/dmlcz/123678

STEWART, Ian. *Galois Theory*. 3. vyd. the United States of America: Chapman & Hall/CRC, 2004. ISBN 1-58488-393-6.

STRNAD, Alois. O pravidelném sedmnáctiúhelníku. *Časopis pro pěstování matematiky a fysiky*. 1904, roč. 33, č. 5, s. 543-558. ISSN: 1802-114X. Dostupné z: http://dml.cz/dmlcz/123514

STUDNIČKA, František Josef. O průběhu života Gaussova. *Časopis pro pěstování matematiky a fysiky*. 1877, roč. 6, č. 4, s. 148-161. ISSN: 1802-114X. Dostupné z: http://dml.cz/dmlcz/123683

TIETZE, Heinrich. *Famous Problems of Mathematics: Solved and Unsolved Mathematical Problems from Antiquity to Modern Times*. Editor: Beatrice Kevitt Hofstadter a Horace Komm. 2. vyd. New York: Graylock Press, 1965. ISBN 1-124-01265-6.